



北京师范大学智慧学习研究院
Smart Learning Institute of Beijing Normal University

Personal Data and Privacy Protection in Online Learning

Guidance for Students, Teachers and Parents

June 2020. Version 1.0



Published by Smart Learning Institute of Beijing Normal University
in partnership with UNESCO IITE & UNESCO INRULED

Personal Data and Privacy Protection in Online Learning: Guidance for Students, Teachers and Parents

© Smart Learning Institute of Beijing Normal University (SLIBNU), 2020

Rights and Permissions



This publication is available in Open Access under the Attribution-ShareAlike 3.0 IGO (CC-BY-SA 3.0 IGO) license (<http://creativecommons.org/licenses/by-sa/3.0/igo/>).

Please cite the work as follows:

Huang, R.H., Liu, D.J., Zhu, L.X., Chen, H.Y., Yang, J.F., Tlili, A., Fang, H.G., Wang, S.F. (2020). Personal Data and Privacy Protection in Online Learning: Guidance for Students, Teachers and Parents. Beijing: Smart Learning Institute of Beijing Normal University.

Personal Data and Privacy Protection in Online Learning: Guidance for Students, Teachers and Parents

Preface

The COVID-19 pandemic has brought unprecedented challenges to our safety, health and education. According to statistics published by UNESCO on 5th April, 1.59 billion students could not go back to school, accounting for 91.3% of the world's student population. After that, the influence of pandemic on education is reduced. Until 13th June, there are 1.11 billion which accounted for 63.3% of the total enrolled student. In this special situation, lots of students have to learn online, because of which a large amount of personal data is shared and also the hidden risks of personal data security are exposed. Personal data and privacy protection have never been so urgent like today, and it has been listed by UNESCO as one of the biggest challenges we are confronting. Therefore, how to protect the personal data and privacy in online learning is becoming an important issue for students, teachers and parents.

In the process of online learning, Personal data are produced through the interaction between students/teachers and tools or platforms. Personal data and privacy are the tranquility of the private life of a natural person, and the private space, private activities, and private information that one is unwilling to be known to others. A privacy policy is a statement or a legal document (in privacy law) that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data. With the large-scale application of online learning, personal privacy protection has become a key issue facing online learning. Many countries and organizations have formulated legislations, regulations and policy documents related to personal data protection. Japan, UK, Australia and other countries, United Nations (UN), Organization for Economic Co-operation and Development (OECD), Asia-Pacific Economic Cooperation (APEC), International Organization for Standardization (ISO) and other organizations also issued a set of personal data protection legislations, regulations, framework and principles.

Recently, the UNESCO Institute for Information Technologies in Education (UNESCO IITE) in partnership with the research team at Tsinghua University has drafted Personal Data Security Technical Guide for Online Education Platforms. The Technical Guide is to outline key recommendations to online education platform providers and relevant education and technical administrators in terms of technical solutions, management as well as awareness raising. However, our guidance book aims to guiding students, teachers and parents to protect personal data and privacy in online learning.

This guidance book systematically sorted out the personal data security risks in online learning, and proposed specific strategies for personal information protection from three aspects: before, during and after learning. In this guidance book, several issues are addressed for personal data and privacy protection for online learning. The publication aims to present the basic ideas on how to protect personal data for online learning and give concrete guidance for learners on specific learning activities, and tries to make the learning environment a smart one for personal data protection.

On behalf of UNESCO IITE and UNESCO INRULED, we would like to thank our partners from the globe. Our special thanks go to the National Commission of the People's Republic of China for UNESCO for their incredible support during the realization of this publication. Thanks also go to those experts from the UNESCO International Research and Training Center for Rural Education (UNESCO INRULED), UNESCO Institute for Information Technologies in Education (UNESCO IITE), International Centre for Higher Education Innovation under the auspices of UNESCO (UNESCO ICHEI). We also acknowledge with gratitude contributions to this publication from our partner organizations, including Smart Learning Institute of Beijing Normal University (SLIBNU), the International Association of Smart Learning Environment (IASLE), the Arab League's Educational, Cultural and Scientific Organization (ALECSO) and Edmodo for their professional feedback and comments during the preparation of this guidance. Last but not the least, we are very thankful to multiple international partners, researchers, and staff worked on developing the contents and organizing the webinar for this guidebook.



Dr. Tao Zhan

Director, UNESCO Institute for
Information Technologies in Educa-
tion




Dr. Ronghuai Huang

Director, UNESCO International
Research and Training Centre for
Rural Education



Acknowledgement

Many people have helped us in finalizing this guidance. They have our great appreciation for the long hours and hard work they devoted to conducting research and developing content. Without their incredible assistance, this book would not have been realized.

We would like to acknowledge the help of several researchers who worked on developing the contents and organizing the webinar for this guidebook, namely Svetlana Knyazeva, Denis Kapelyushnik, Ting-Wen Chang, Hongyan Kuai, Mushen Deng, Jiajia Liu, Shichong Wang, Jinchao Su, Hongjin He, Ruiheng Zhao, Liuxia Pan. We would like also to acknowledge the contribution of multiple international partners, researchers, and staff who provided new ideas for this guidebook during the organized webinar.

Thanks also go to those experts from the Smart Learning Institute of Beijing Normal University (SLIBNU), UNESCO International Research and Training Center for Rural Education (UNESCO INRULED), UNESCO Institute for Information Technologies in Education (UNESCO IITE), International Centre for Higher Education Innovation under the auspices of UNESCO (UNESCO ICHEI), International Association of Smart Learning Environments (IASLE), Arab League's Educational, Cultural and Scientific Organization (ALECSO) and Edmodo for their professional feedback and comments during the preparation of this guidance.

Contents

Executive Summary	
Chapter 1 Realizing the Urgency for Personal Data Protection in Online Learning	1
1.1 Online learning and personal data	1
1.2 Personal data protection for students	4
1.3 Legislation and regulation on data protection	7
Chapter 2 Understanding Personal Data and Privacy during Learning Online	11
2.1 Personal data and their lifecycle	11
2.2 Student data and privacy	17
2.3 Privacy frameworks and principles	22
2.4 Data collected in online learning	26
2.5 Students and parents' rights to data	28
Chapter 3 Preparing Devices, Network, and Tools	31
3.1 Setting up your device	31
3.2 Managing network connection on your device	32
3.3 Selecting and installing learning tools	34
3.4 Browsing the privacy policy	36
Chapter 4 Preserving Privacy when Signing up/in on Learning Platforms	40
4.1 Using strong passwords to create accounts	40
4.2 Signing in a device that's not yours	45
Chapter 5 Protecting Privacy when Navigating Learning Platforms	49
5.1 Enrolling in an online course	50
5.2 Utilizing personalized learning services	52
5.3 Using search services carefully	53
5.4 Recognizing location services	56
5.5 Backing up your data	57
Chapter 6 Staying Safe while Learning with Social Networking Service	60
6.1 Using video conference tools with caution	63
6.2 Posting in forums responsibly	65
6.3 Surfing the Internet safely	66
Chapter 7 Clearing Personal Data after Learning Online	77
7.1 Removing data traces in online learning	77
7.2 Deactivating your account	80
Conclusion	84
Reference	86
Glossary	93
Index of Topics	96

Executive Summary

With COVID-19 spreading, lots of students have to learn online. In fact, online learning is generally becoming a norm for everyone to become a life-long learner. Therefore, how to protect the personal data and privacy in online learning is becoming an important issue for students, parents, and administrators. In order to protect personal data and privacy, students should understand how the personal data are produced when they are learning online, and how to preserve the privacy.

In this guidance book, several issues are addressed for personal data and privacy protection when learners are learning online.

First, online learning and the typical learning activities are presented and the personal data generated in the learning process are described. The legislations, regulations and policy of personal data protection for children are also tabled in the content. The overall legislations and regulations on personal data protection are also listed. It is urgent for students to protect their personal data in online learning.

The second chapter details the definition and constitutes of personal data and privacy, especially the lifecycle of online personal data. The characteristics of student data and the privacy are also articulated. The privacy framework and principles are also listed. Then the data collected in online learning and the rights for students and parents for the data are discussed.

From chapter 3 to chapter 7, the concrete activities for protecting personal data are introduced. Chapter 3 deals with the issues before online learning, such as setting up the personal digital devices, managing network settings, selecting and installing online learning tools, etc. Chapter 4 mainly discusses the how to preserve personal data when signing up/in on online learning platforms. Chapter 5 is essential for online learner for protecting personal privacy, by rethinking the learning activities of joining a course, utilizing the personal learning services, recognizing local services, and backing up the learning data. Chapter 6 mainly focuses on keep personal data safe by utilizing social software tools, such as surfing online, using webinar, and posting in forums. Chapter 7 concerns how to clear personal data after finishing online learning.

The guidance book aims to present the basic ideas on how to protect personal data for online learning and give concrete guidance for learners on specific learning activities. Let's try to make the learning environment a smart one for personal data protection.

Chapter 1 Realizing the Urgency for Personal Data Protection in Online Learning

1.1 Online learning and personal data



Term: Online learning

Online learning is defined as learning experiences in synchronous or asynchronous environments using different devices (e.g., mobile phones, laptops, etc.) with internet access. In these environments, students can be anywhere (independent) to learn and interact with instructors and other students (Singh and Thurman, 2019).

In online learning, the essence of interaction among students, teachers, and content is well understood and is referenced in many theories of education. Terry Anderson's Online Learning Model (2011) illustrates the interactions among the three elements, and can help us to deepen our understanding of complex educational context.

Students can choose to have their own learning sequenced, directed, and evaluated with the assistance of a teacher. This interaction can take place within a community of inquiry, using a variety of internet-based synchronous and asynchronous activities (video, audio, computer conferencing, chats, or virtual world interaction). These synchronous and asynchronous online environments will promote the development of social and collaborative skills, as well as personal relationships among participants.

Students can also interact directly with the learning content that they find in multiple formats. The second model of learning illustrates the structured learning tools (simulations, games, virtual labs, etc.) associated with independent learning. It should also be emphasized, however, the student is not alone. Often peers located locally or distributed across the Net, formal and informal groups, and parents, have been significant sources of support and assistance to independent study students (Potter, 1998).

(1) Categories of online learning tools

Effectively selecting and using learning tools is beneficial to learners in finding and processing information, constructing knowledge, collaborating with peers, expressing understanding and evaluating learning effects in concrete ways. The convenience of tools should be taken into consideration when choosing learning scenarios. Specifically, tools should be convenient and quick to: (a) help teachers effectively produce and manage resources, release notices and manage students; (b) help students obtain resources, participate in learning activities; (c) help teachers and students interact in real time; and, (d) help teachers, parents and schools understand students' learning performance and make timely school-home interaction. In order to facilitate teachers at all levels to quickly select various learning tools for a smooth online teaching, learning tools are divided into eight categories, as shown below:

- Tools for resources producing, including PPT recording software, screen capture software and the software of video production and multimedia learning resources producing, etc.
- Tools for synchronous live teaching, including software on interactive teaching, remote offline, on-line-course
- Tools for asynchronous teaching, including all kinds of online teaching platforms national level, regional level and university community level, as well as those launched by universities and enterprises
- Tools for self-regulated learning, including learning apps for all subjects
- Tools for knowledge construction, including cognitive tools, collaborative editing tools, virtual simulation tools, etc.
- Tools for learning analytics, including apps, websites, and interactive class software supporting data analysis
- Tools for practice and evaluation, including all kinds of tools suitable for conducting practice and the evaluation of learning results
- Tools for resources and class management, including all kinds of tools suitable for the effective organization of online learning with abundant learning resources, a large number of students and learning tasks

(2) Typical steps for online learning

When considering data protection in online learning, it is important to know the typical steps for using multitype online learning tools.

1) Preparing devices, network, and tools

Before learning online, preparing the devices, networking, tools, and reading privacy policy are basic aspects for personal data protection, which can guarantee the quality of online learning.

- Setting up your device
- Managing network connection on your device
- Selecting and installing learning tools
- Browsing the privacy policy

2) Preserving privacy when signing up/in on learning platforms

When signing in on any learning platforms, the first and most important behavior is to register in the platform, however, the importance is often ignored by users which leads to forget the username/password, leak password,

or other issues.

- Using strong password to create account
- Signing in a device that's not yours

3) Protecting privacy when navigating learning platforms

After signing in on a learning platform, learners could enroll in the courses, post messages in forums, blogs, browse and learn the contents. This section will introduce the issues associated with the personal data protection in navigating learning platforms.

- Enrolling in an online course
- Utilizing personalized learning services
- Using search services carefully
- Recognizing location services
- Backing up your data

4) Staying safe while learning with social networking

Social networking tools are increasingly being used in online learning, providing students with a medium in which they can actively engage with each other and with their teachers, co-create knowledge, share experiences, work and learn collaboratively. However, the use of social networks among students may affect their academic life negatively. This is buttressed by the fact that the personal data may leak in social network, their use constitutes distractions, as well as that the students tend to invest a good deal of time in the use of such technologies.

- Using video conference tools with caution
- Posting in the discussions and forums responsibly
- Surfing the Internet safely

5) Clearing personal data after learning online

After finishing online learning in period, the user should notice the data generated as discussed in the previous chapters, and make the decision on whether to delete the data or not. If you decide to delete the data, the following section provide some suggestions and methods.

- Removing data traces in online learning
- Deactivating your account

1.2 Personal data protection for students

In the process of online learning, data are produced through the interaction between students/teachers and tools or platforms. In most scenarios, students/teachers may not have the awareness to protect their personal data. However, with the infusion of Internet with education, it is vital for the users to have basic data literacy, including data and privacy protection.

Personal data privacy and personal data protection are very closely interconnected. Privacy concerns arise wherever data is collected, stored, or used. Privacy is about authorized access – who has it and who define it. Data privacy is focused on the use and governance of personal data – things like putting policies in place to ensure that users' personal information is being collected, shared and used in appropriate ways.

David Flaherty (1989) believes networked computer databases pose threats to privacy. He develops 'data protection' as an aspect of privacy, which involves “the collection, use, and dissemination of personal information”. This concept forms the foundation for fair information practices used by governments globally.

With the development of Internet, many countries and organizations have formulated legislations, regulations and policy documents related to personal data protection, as shown in table 1-1. Special protective measures have been taken for students and children. In addition, social organizations and enterprises have taken different measures to ensure the security of personal data.

Table 1-1 Legislation and regulation on students and children

Legislation or Regulation	Country or Organization	Release Date	Child Definition	Details
Children's Online Privacy and Freedom of Expression	United Nations International Children's Emergency Fund (UNICEF)	2018	Under 18	The Guidelines for Industry on Child Online Protection, published by UNICEF and the International Telecommunications Union in 2015, further explore the corporate responsibility to respect children's rights in a digital world. This Toolkit builds on these Guidelines, expanding the consideration of children's rights to privacy and freedom of expression. It identifies five overarching principles, based in international human rights law, that should ground and shape decisions about children online.

Legislation or Regulation	Country or Organization	Release Date	Child Definition	Details
Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment	Council of Europe	2018	Under 18	Children have a right to private and family life in the digital environment, which includes the protection of their personal data and respect for the confidentiality of their correspondence and private communications. States must respect, protect and fulfil the right of the child to privacy and data protection. States should ensure that relevant stakeholders, in particular those processing personal data, but also the child's peers, parents or carers, and educators, are made aware of and respect the child's right to privacy and data protection.
K-12 Cybersecurity Act	US	2019	From kindergarten to 12th grade	The K-12 Cybersecurity Act of 2019 would help educational institutions bolster their cybersecurity protections by instructing the Department of Homeland Security (DHS) to examine the risks and challenges that schools face in securing their systems.
Provisions on the Cyber Protection of Children's Personal Information	China	2019	Under 14	No network operator shall collect any child's personal information irrelevant to the services provided by it, or collect such information in violation of laws, administrative regulations or the agreement of both parties.

Among the privacy protection for each group, the student group should be more concerned. On the one hand, because of learning and education needs, students will generate a lot of personal data in the course of studying, such as name, address, home address, test scores, behavioral events, and so on. On the other hand, in order to facilitate the management, the school collects many students' personal information. If this information is not protected, it will be easily leaked and used by criminals.

Many countries and regions will formulate laws and regulations to protect students' data and privacy. Still, the relevant laws and regulations are usually a few items in a general law, and there are rarely separate legislations for student privacy protection. However, some organizations and schools have issued regulations and guidelines to guide and help data protection for students' parents and teachers by adapting to the laws of their own countries.

Further Reading

Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children's Privacy Law

Google and its subsidiary YouTube will pay a record \$170 million to settle allegations by the Federal Trade Commission (FTC) and the New York Attorney General that the YouTube video sharing service illegally collected personal information from children without their parents' consent.

The settlement requires Google and YouTube to pay \$136 million to the FTC and \$34 million to New York for allegedly violating the Children's Online Privacy Protection Act (COPPA) Rule. The \$136 million penalty is by far the largest amount the FTC has ever obtained in a COPPA case since Congress enacted the law in 1998.

In a complaint filed against the companies, the FTC and New York Attorney General allege that YouTube violated the COPPA Rule by collecting personal information—in the form of persistent identifiers that are used to track users across the Internet—from viewers of child-directed channels, without first notifying parents and getting their consent. YouTube earned millions of dollars by using the identifiers, commonly known as cookies, to deliver targeted ads to viewers of these channels, according to the complaint.

The COPPA Rule requires that child-directed websites and online services provide notice of their information practices and obtain parental consent prior to collecting personal information from children under 13, including the use of persistent identifiers to track a user's internet browsing habits for targeted advertising. In addition, third parties, such as advertising networks, are also subject to COPPA where they have actual knowledge, they are collecting personal information directly from users of child-directed websites and online services.

The YouTube platform allows Google account holders, including large commercial entities, to create "channels" to display their content. According to the complaint, eligible channel owners can choose to monetize their channel by allowing YouTube to serve behaviorally targeted advertisements, which generates revenue for both the channel owners and YouTube.

In the complaint, the Federal Trade Commission (FTC) and New York Attorney General allege that while YouTube claimed to be a general-audience site, some of YouTube's individual channels—such as those operated by toy companies—are child-directed and therefore must comply with COPPA.

The complaint notes that the defendants knew that the YouTube platform had numerous child-directed channels. YouTube marketed itself as a top destination for kids in presentations to the makers of popular children's products and brands. For example, Google and YouTube told Mattel, maker of Barbie and Monster High toys, that "YouTube is today's leader in reaching children age 6-11 against top TV channels" and told Hasbro, which makes My Little Pony and Play-Doh, that YouTube is the "#1 website regularly visited by kids."

1.3 Legislation and regulation on data protection

With the development of Internet, many countries and organizations have formulated legislations, regulations and policy documents related to personal data protection, as shown in table 1-2. In addition, social organizations and enterprises have taken different measures to ensure the security of personal data.

Generally, laws that protect the individual tend to be expressed in national laws that are particular to each country's characteristics. These national laws are also the best way to translate general principles - including transnational data protection principles - to the particularities of a certain country's legal system. The core of international data protection laws is the presence of principles such as the Fair Information Privacy Principles.

European Union

The European Union is based on the respect for fundamental rights. The European Convention on Human Rights and Article 8 of the Charter of Fundamental Rights of the European Union expressly recognizes the fundamental right to the protection of personal data. For several years, law enforcement agencies in various countries have urged the adoption of "data retention" requirements, which would compel communications service providers to routinely capture and archive information detailing the telephone calls, e-mail messages and other communications of their users. While many providers currently retain certain traffic data for billing and other business-related purposes for short periods of time, there are no government-imposed retention requirements in the major industrialized countries. In 2018, European Union issued the world's strictest personal information protection law, known as General Data Protection Regulation (GDPR).

United States

Following the enactment of the Privacy Act in 1974, the US has enacted special legislation in the fields of finance, consumer protection and child discipline, such as The Children's Online Privacy Protection Act (COPPA), The Protection of Pupil Rights Amendment (PPRA), K-12 Cybersecurity Act of 2019, etc.

China

In China, State Council approved the Administrative Measures for the Security Protection of Computer Information Networks Linked to the Internet on December, 1997, these measures are formulated with a view to strengthening the security protection of the International networking of computer information networks and maintaining public order and social stability. In 2017, Cybersecurity Law was implemented, stipulating the general objectives and basic principles of the cyber information security law. The Provisions on the Cyber Protection of Children's Personal Information of 2019 marks a new step forward in China's efforts to secure the Internet and protect the privacy of individuals, especially children.

Other countries and international organizations

Japan, UK, Australia, Brazil, South Africa and other countries, United Nations (UN), Organization for Economic Co-operation and Development (OECD), Asia-Pacific Economic Cooperation (APEC), International Organization for Standardization (ISO) and other organizations also issued a set of personal data protection legislations, regulations, framework and principles.

Table 1-2: Legislation and regulation of countries and organizations

Legislation or Regulation	Country or Organization	ReleaseDate	Details
68/167. The Right to Privacy in the Digital Age	United Nations (UN)	2013	Affirmed that the rights held by people offline must also be protected online, and it called upon all States to respect and protect the right to privacy in digital communication.
General Comment No. 16 Article 17	United Nations' Human Rights Committee (UNHRC)	1988	The right to respect of privacy, family, home and correspondence, and protection of honour and reputation
Guidelines on the Protection of Privacy and Transborder Flows of Personal Data	Organization for Economic Co-operation and Development (OECD)	1980	The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data.
ISTE Standards for Education Leaders, Educators, and Students	The International Society for Technology in Education (ISTE)	1998	The ISTE Standards are a framework for innovation in education. These standards help educators and education leaders worldwide prepare learners to thrive in work and life.
NIST SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)	The National Institute of Standards and Technology — agency of the United States Department of Commerce (NIST)	2010	The purpose of this document is to assist Federal agencies in protecting the confidentiality of personally identifiable information (PII) in information systems. The document explains the importance of protecting the confidentiality of PII in the context of information security and explains its relationship to privacy using the Fair Information Practices, which are the principles underlying most privacy laws and privacy best practices. PII should be protected from inappropriate access, use, and disclosure.
ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework	International Organization for Standardization (ISO)	2011	This International Standard provides a high-level framework for the protection of personally identifiable information (PII) within information and communication technology (ICT) systems.

Legislation or Regulation	Country or Organization	ReleaseDate	Details
General Data Protection Regulation (GDPR)	European Union (EU)	2018	The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.
The Privacy Act	United States	1974	The Privacy Act of 1974, a United States federal law, establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.
Cybersecurity Law	China	2016	This Law is developed for the purposes of guaranteeing cybersecurity, safeguarding cyberspace sovereignty, national security and public interest, protecting the lawful rights and interests of citizens, legal persons and other organizations, and promoting the sound development of economic and social informatization.
Act on the Protection of Personal Information	Japan	2003	The Personal Information Protection Act (Law No. 57 of 2003) (hereinafter referred to as "Act"), which was promulgated on May 23, 2003, became fully effective on April 1, 2005, as to the private sector.
Protection of Personal Information Bill	South Africa	2009	This Bill seeks to support the right to privacy of personal information of South African citizens and bring South Africa in line with international data protection laws. The Bill protects the personal information collected and processed by organizations.

Legislation or Regulation	Country or Organization	ReleaseDate	Details
Data Protection Act	United Kingdom	2018	The Data Protection Act 1998 was a United Kingdom Act of Parliament designed to protect personal data stored on computers or in an organized paper filing system. It enacted the EU Data Protection Directive 1995's provisions on the protection, processing and movement of data. It was superseded by the UK Data Protection Act 2018.
Personal Information Protection and Electronic Documents Act	Canada	2019	Under PIPEDA, personal information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form.

Chapter 2 Understanding Personal Data and Privacy during Learning Online

2.1 Personal data and their lifecycle



Term: Personally Identifiable Information (PII)

Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

– NIST SP 800-122 *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*

Personal data, also known as personal information or personally identifiable information (PII) is any information relating to an identifiable person. The abbreviation PII is widely accepted in the United States. However, under European and other data protection regimes, which center primarily around the General Data Protection Regulation, the term “personal data” is significantly broader, and determines the scope of the regulatory regime. The comparison of the definition on personal data could be found in table 2-1.

The concept of personal data has become prevalent as information technology and the Internet have made it easier to collect, leading to a profitable market in collecting and reselling personal data. Personal data can also be exploited by criminals to stalk or steal the identity of a person, or to aid in the planning of criminal acts. As a response to these threats, lawmakers of various countries have enacted a series of legislation to limit the distribution and accessibility of personal data.

Table 2-1: Comparison of definition on personal data from different countries

Legislation or Regulation	Country or Organization	Definition of Personal Data
ISO/IEC 29100:2011	United Nations (UN)	Affirmed that the rights held by people offline must also be protected online, and it called upon all States to respect and protect the right to privacy in digital communication.
Information technology — Security techniques — Privacy framework	International Organization for Standardization (ISO)	Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.
Personal Data: The Emergence of a New Asset Class	The World Economic Forum	Personal data is defined as data (and metadata) created by and about people, encompassing: • Volunteered data – created and explicitly shared by individuals, e.g., social network profiles. • Observed data – captured by recording the actions of individuals, e.g., location data when using cell phones. • Inferred data – data about individuals based on analysis of volunteered or observed information, e.g., credit scores.
General Data Protection Regulation (GDPR)	European Union	Personal data means any information relating to an identified or identifiable natural person (data subject)
NIST SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)	United States	Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
Cybersecurity Law of the People's Republic of China	China	Personal information refers to all kinds of information recorded by electronic or other means that can identify the personal identity of a natural person independently or in combination with other information, including but not limited to the name, date of birth, ID number, personal biometric information, address, telephone number, etc. of a natural person.

(1) Categories of personal data

Personal data is a complex concept, which includes many categories. Understanding the classification of personal data can help increase awareness of the protection of personal data and clarify the methods of personal data protection.

Many countries or international organizations have classified personal data. In fact, these classifications are quite similar. Among them, some classification methods divide personal data into two levels, and some classification methods divide personal data into three levels.

According to Institute of Electrical and Electronics Engineers (IEEE) publication Ethically Aligned Design: A Vision for Prioritizing Human Wellbeing with Artificial Intelligence and Autonomous Systems, digital persona is fictitious characters created to represent the different user types that might use a site or product, as shown in Figure2-1. It includes health data, government data, education data, transport data, immigration data, consumer and loyalty data, telecommunications data, media and content data, tax and employment data, online forums, voting and party affiliation data, insurance and legal data, banking and finance data and digital inheritance data.

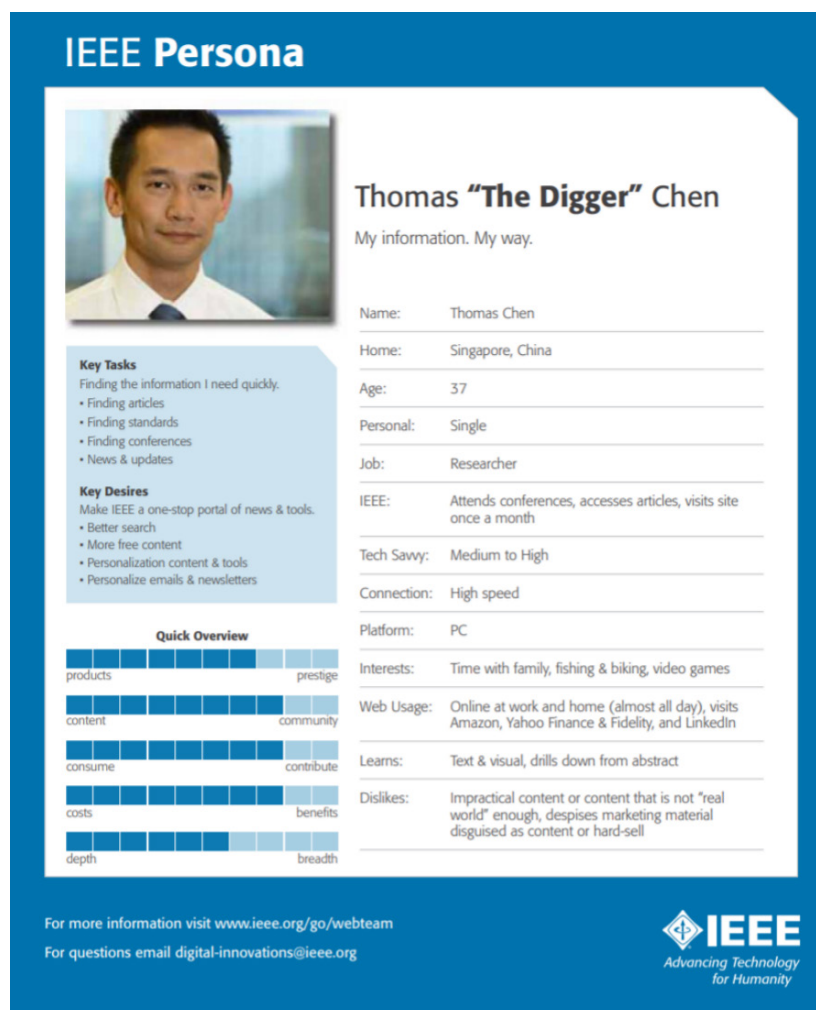


Figure 2-1: An IEEE persona

International Association of Privacy Professionals (IAPP) divides personal data (personal information) into three levels and six primary categories: “internal, external, historical, financial, social, and tracking”. These six categories have 24 secondary categories.

In the “Information Security Technology - Personal Information Security Specification” issued by the Chinese government, personal data is divided into two levels (personal information, personal sensitive information) and 13 more detailed categories. The classification of California Consumer Privacy Act (CCPA) of US is more biased towards personal information related to consumption and purchase behavior.

Basically, personal identification data, financial data, health data and other categories can be seen in all classifications. Still, the content which related to personal social life and personal tracking information is not available in some classification methods. Combining the different characteristics and commonalities of various classification methods, we summarize the methods adopted to classify personal data, as shown in table 2-2.

Table 2-2: Categories of personal data

Basic information	Name, age, place of birth, date of birth, gender, gender identity, preferences, proclivities, personal photos, race, color, national or ethnic origin
Identification	Government-issued identification, driver's license, passport, health IDs, Social Insurance Numbers (SIN), Social Security Numbers (SSN), PIN numbers
Biometrics	Genes, fingerprints, voice prints, palm prints, auricles, irises, facial features
Authenticating	Passwords, PIN, system account, IP address, email address, security answer, personal digital certificates
Medical and Health	Physical and mental health, drug test results, disabilities, family or individual health history, health records, blood type, DNA code, medical history, medical device logs, prescriptions, and health insurance coverage
Professional	Job titles, salary, work history, school attended, education history, employee files, employment history, evaluations, references, interviews, employer data, certifications, disciplinary actions

Financial	Cars, houses, apartments, personal possessions, purchases, sales, credit, income, loan records, transactions, taxes, purchases and spending habits, credit records, credit scores, credit standing, credit capacity, physical assets, and virtual goods
Communication	Telephone recordings, voice mail, emails, SMS, phone calls, IM and social, network post, physical address, telephone number
Contact	Contact lists, friends, connections, acquaintances, associations, group membership, email address
Browsing history	Media produced, consumed, and shared: in-text, audio, photo, video, and other forms of media; Real-world and online context, activity, interests, and behavior: records of location, time, clicks, searches, browser histories and calendar data, purchases activity, online shopping, social network profile information and the like
Device	Hardware serial number, software list, IP address, Mac address, browser fingerprint
Location	Country, GPS coordinates, room number, longitude and latitude

(2) Lifecycle of online personal data

The data lifecycle is the sequence of stages that a particular unit of data goes through from its initial generation or capture to its eventual archival and/or deletion at the end of its useful life. According to the Personal Data Security Technical Guide for Online Education Platforms published by the UNESCO Institute for Information Technologies in Education (UNESCO IITE), data lifecycle includes 5 stages as data collection, data transmission, data usage, data storage and data destruction.

1) Collection

The data collection performed by the online education platform should comply with the security principles and providing classification and category of the data according to data attributes such as of types, sensitivities. The online education platform should have the consent or authorization of a guardian when collecting and using information of juveniles. When data is marked as PII or information related to a PII body, the online education platform should implement privacy security controls.

2) Transmit

To ensure data transmission security, the online education platform should establish an appropriate protection mechanism in the process of data transmission, and use network security protocols such as TLS, IPsec, etc., and use cryptography algorithms recommended by the relevant standards.

3) Use

Online education platforms should provide unified rights management to ensure that users apply and access relevant data on demand in accordance with the principle of least privilege. The online education platform should provide comprehensive security monitoring and access auditing measures for the use and access of relevant data, as well as PII protection mechanisms (including but not limited to privacy protection technologies such as de-identification and pseudo-anonymization technologies).

4) Storage

The online education platform's data storage should comply with the security principles and be protected by access control and security protection to prevent unauthorized access, modification, destruction, removal, or other use. Such mechanisms include, but are not limited to, encryption, signature, anonymization, key management, etc. The online education platform should have the capabilities of high availability, data backup and disaster recovery to ensure reliability and availability of the data.

5) Destroy

The online education platform should destroy the data according to the data classification and storage media. Before information processing facilities and storage media are removed from the online education platform, data removal and physical destruction should be carried out in accordance with relevant standards to avoid the risk of data leakage.

Further Reading

Know better about your personal data

Every day, you need to provide your data. Give your identification documents and contact details to your employer, or the name of your kids and other information to their school, or your medical history to doctors, or your IP to get your location and obtain directions, and so on.

The solution is not to start living in a cave; on the contrary, you should keep on doing your daily activities but paying attention to what you are sharing, to who you are giving access and how is the store and dispose of securely.



Figure 2-2: How to protect your personal data

2.2 Student data and privacy

Student data, in education, refers to any information that educators, schools, districts, and online services collect on individual students, which is a kind of student's education record. High-quality education data are essential for improving students' achievement in school and preparing them for success in life. When effectively used, these data can empower educators, students, and families with the information they need to make decisions to help all learners succeed.



Term: Education record

“Education records” are records that are directly related to a student and that are maintained by an educational agency or institution or a party acting for or on behalf of the agency or institution. These records include but are not limited to grades, transcripts, class lists, student course schedules, health records (at the K-12 level), student financial information (at the postsecondary level), and student discipline files. The information may be recorded in any way, including, but not limited to, handwriting, print, computer media, videotape, audiotape, film, microfilm, microfiche, and e-mail.

– 34 CFR § 99.2, *Family Educational Rights and Privacy Act of United States*

(1) What constitutes student data?

Traditionally, student data consisted of things like attendance, grades, discipline records, and health records. Access to that data used to be restricted to the administrator, guidance counselor, teacher, or other school official who needed it to serve the educational needs of the child.

With the use of technology in schools, traditional data is now often shared with companies that provide Student Information Systems (SIS), Learning Management Systems (LMS), and many other technologies. Parents, students, and others have raised concerns about what information is being collected or shared, and what use those companies might make of that data.

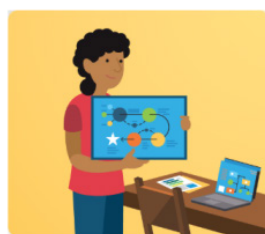
Student personal information includes any information about a student’s identity, academics, medical conditions, or anything else that is collected, stored, and communicated by schools or technology vendors on behalf of schools that is particular to that individual student. This include:

- Name
- Contact details, contact preferences, date of birth, identification documents
- Parental, sibling and extended family details
- Children who are adopted from care, looked after children, under special guardianship
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, language, eligibility for free school meals, Pupil Premium or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers

- Photographs of your child
- Carefully chosen and vetted educational apps
- CCTV images

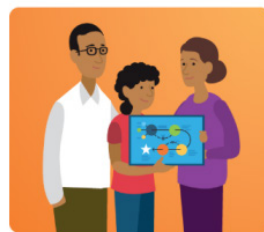
(2) What is the value of student data?

Data is one of the most powerful tools to inform, engage, and create opportunities for students along their education journey—and it's much more than test scores. Data helps us make connections that lead to insights and improvements, as shown in Figure 2-3. Student data helps a student to know better of his/her learning style and ability and to shape his/her own education journey. Student data helps parents to know what actions to take to help their children on the path to success. Student data helps teachers know where their students are succeeding and struggling right now, so teachers can help accordingly. Student data helps school leaders to know what's working and what isn't in school, so school leaders can make timely decisions and make sure resources support great teaching and improve student learning. Student data also help afterschool partners to know what's happening with students before school, so they can help families and communities create more opportunities for students to succeed.



Students

"I know my strengths and where I need to grow. I can shape my own education journey."



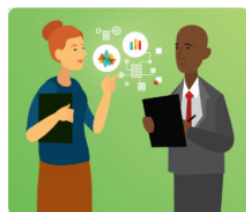
Parents

"I know what actions to take to help my child on her path to success. I can be a better champion for her."



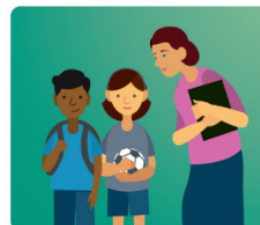
Teachers

"I know where my students are succeeding and struggling right now. I can help them grow."



School Leaders

"I know what's working and what isn't in my school. I can make timely decisions and make sure resources support great teaching and improve student learning."



Afterschool Partners

"I know what's happening with these kids before 3:00 p.m. I can help families and communities create more opportunities for students to succeed."

Figure 2-3: The value of student data to stakeholders

Data has the potential to transform education into a personalized experience that meets the needs of individuals and ensures that no student is lost along the way. From parents to policymakers, education stakeholders use different types of data—including test scores, course grades, and demographic information—in different ways to improve education for students.

Further Reading

Foundational Principles for Using and Safeguarding Students' Personal Information

1. Student data should be used to further and support student learning and success.
2. Student data are most powerful when used for continuous improvement and personalizing student learning.
3. Student data should be used as a tool for informing, engaging, and empowering students, families, teachers, and school system leaders.
4. Students, families, and educators should have timely access to information collected about the student.
5. Student data should be used to inform and not replace the professional judgment of educators.
6. Students' personal information should only be shared, under terms or agreement, with service providers for legitimate educational purposes; otherwise the consent to share must be given by a parent, guardian, or a student, if that student is over 18. School systems should have policies for overseeing this process, which include support and guidance for teachers.
7. Educational institutions, and their contracted service providers with access to student data, including researchers, should have clear, publicly available rules and guidelines for how they collect, use, safeguard, and destroy those data.
8. Educators and their contracted service providers should only have access to the minimum student data required to support student success.
9. Everyone who has access to students' personal information should be trained and know how to effectively and ethically use, protect, and secure it.

(retrieved from <https://studentdataprinciples.org/the-principles/>)

(3) Student data privacy



Term: Privacy

Privacy is the tranquility of the private life of a natural person, and the private space, private activities, and private information that one is unwilling to be known to others.

– Article 1032, Civil Code of the People's Republic of China

Broadly speaking, privacy is the right to be let alone, or freedom from interference or intrusion. Information privacy is the right to have some control over how your personal information is collected and used.

According to the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of Organization for Economic Co-operation and Development (OECD), there has been a tendency to broaden the traditional concept of privacy (“the right to be left alone”) and to identify a more complex synthesis of interests which can perhaps more correctly be termed privacy and individual liberties.

In specific, privacy may be divided into four categories (1) Physical: restriction on others to experience a person or situation through one or more of the human senses; (2) unknowable to others; (3) Decisional: restriction on interfering in decisions that are exclusive to an entity; (4) Dispositional: restriction on attempts to know an individual's state of mind.

Student data privacy covers the use, collection, handling and governance of students’ personally identifiable information (PII). This includes any and all information that can be used to identify, locate or contact an individual student.

Everyone who uses student data has a responsibility to maintain students’ privacy and the security of their data, especially when these data are personally identifiable. This starts with limiting the data that are collected, stored, shared, and used to support student learning and success. Whenever possible, aggregated, de-identified data that do not identify individual students should be used to inform key policy decisions and help improve services and systems that benefit students. In instances where using personal data is necessary, those few individuals who have access to this information to carry out their duties must handle it in a legal, responsible, and ethical manner.

The subject of student data privacy has never been more relevant, important, and stress inducing for school administrators. Although the topic has been around since the 1970s, when schools began collecting electronic information, a lot has changed since the days of analog technologies and magnetic tapes. The size of our data universe has exploded, and most schools today are relying on cloud services to collect and store their data. The risks and responsibilities on administrators, as it relates to student data privacy, have never been greater.

Student data privacy is important because there are legal and ethical limitations on the collection, use, sharing, and handling of student PII. Federal and state laws regulate the privacy of student PII—and while enforcement has been historically lax, the legal landscape is changing. Meanwhile, data collection and the use of student information inside and outside our schools is rising all the time. Plus, administrators are outsourcing data services and bringing more technology into the classroom, resulting in a greater number of contracts with information technology (IT) service and solution providers—and more for schools to manage. This evolution should serve as a wake-up call for all administrators. The bottom line is that schools are legally and ethically obligated to keep student PII private - regardless of where and how the student data is created, used, or stored.

2.3 Privacy frameworks and principles



Term: Privacy Policy

A privacy policy is a statement or a legal document (in privacy law) that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data. Personal information can be anything that can be used to identify an individual, not limited to the person's name, address, date of birth, marital status, contact information, ID issue, and expiry date, financial records, credit information, medical history, where one travels, and intentions to acquire goods and services.

– McCormick, Michelle. "New Privacy Legislation." *Beyond Numbers* 427 (2003): 10-. ProQuest. Web. 27 Oct. 2011

With speed-of-light technological innovation, privacy is becoming more complex by the minute as more data is being collected and exchanged. As the technology gets more sophisticated (indeed, invasive), so do the uses of data. And that leaves organizations such as online learning tools provider facing an incredibly complex risk matrix for ensuring that personal information is protected.

Organizations are required to implement "appropriate technical and organizational measures" to secure the personal data they process by privacy laws and regulations. They must also follow the accountability principle. This means being responsible for, and able to demonstrate their compliance with, the law's data processing principles.

This can best be achieved via a privacy compliance framework: a formal structure for managing the security of personal data. The basic structure of these frameworks and principles consist of 3 parts: purpose, scope and principles.

United Nations (UN) Personal Data Protection and Privacy Principles were developed and finalized by the inter-agency UN Privacy Policy Group (PPG) consisting of 30 UN agencies, over a course of two years. UNESCO has joined and contributed to the PPG since the UN Global Pulse initiated in late 2016, in line with its global mandate of promoting Internet Universality ROAM framework (human Rights, Openness, Access, Multi-stakeholder).

These Principles aim to:

- Harmonize standards for the protection of personal data across the UN System
- Facilitate the accountable processing of personal data for the purposes of implementing the mandates of the United Nations System Organizations
- Ensure respect for the human rights and fundamental freedoms of individuals, in particular the right to privacy

These Privacy Principles have high relevance in view of the increasing recognition by the Member States of the role that the protection of the right to privacy plays in utilizing data and technology for the achievement of the 2030 Agenda for Sustainable Development Goals.

UNESCO stands strong to promote these Principles globally and within the Organization and has a particular mandate in education and capacity building dimension. Privacy and personal data protection are part of the Digital Skills UNESCO promotes. At the institutional level, UNESCO has already agreed to integrate these Principles into UNESCO policy, with further guidelines being developed for the Organization to protect personal data and privacy in carrying out its mandate and daily work.

Except for United Nations (UN) Personal Data Protection and Privacy Principles, Organization for Economic Co-operation and Development (OECD) Privacy Framework, Asia-Pacific Economic Cooperation (APEC) Privacy Framework, American Institute of Certified Public Accountants (AIPCA) Generally Accepted Privacy Principles (GAPP), International Organization for Standardization (ISO) 27701 Privacy Information Management System (PIMS) are the typical principles, and the 5 domains mapped from these principles are shown in table 2-3.

According to table 2-3, a proper privacy policy should cover:

- The clear and easily accessible statements (Transparency)
- The types of information collected by the website or app (Limited Collection & Use)
- Data storage and use (Data Lifecycle Management)
- How data are protected (Security by Design)
- How user can manage their data (Data Subject Rights)

Table 2-3: Domains of typical frameworks and principles

Domains	Description	UN	OECD	APEC	GAPP	ISO 27701
Transparency	Provide a transparent notice to the public about privacy practices through a clear and conspicuous notice	Transparency	Openness	Notice	Notice	Openness, Transparency and Notice
Limited Collection & Use	Ensure that the design of information collections is consistent with the intended use of the information, and the need for new information is balanced against any privacy risks.	Proportionality and Necessity	Collection Limitation	Collection Limitation	Collection	Collection Limitation
						Data Minimization
Data Lifecycle Management	Limit the collection, creation, use, dissemination, maintenance, retention, and/or disclosure of personal data	Purpose Specification	Purpose Specification	Use of Personal Information	Use, Retention and Disposal	Purpose Legitimacy and Specification
			Use Limitation		Disclosure to Third Parties	Use, Retention and Disclosure Limitation
Security by Design	Establish administrative, technical, and physical safeguards to protect sensitive data	Security	Security Safeguards	Security Safeguards	Security for Privacy	Information Security
Data Subject Rights	Provide individuals with appropriate access to their personal data.	Fair and Legitimate Processing	Individual Participation	Access and Correction	Access	Individual Participation and Access

Further Reading

Consent Management Platform (CMP)

Consent management is a process which allows websites to meet the law or regulatory requirements regarding consent collection. With a consent-management platform (CMP) in place, websites have the technical capability to inform visitors about the types of data they'll collect and ask for their consent for specific data-processing purposes. CMP offers a set of privacy assurance programs that enable organizations that collect or process personal information to demonstrate responsible data collection and processing practices consistent with regulatory expectations and external standards for privacy accountability. Below are five common consent management platforms.



Piwik PRO emphasizes adherence to the strictest privacy standards on both sides of the Atlantic, whether it's the GDPR or HIPAA. Incorporated in 2013, Piwik PRO is a portfolio company of custom AdTech software house Clearcode. It supports data-sensitive customers from banks to public sector organizations.



TrustArc (formerly known as TRUSTe) is a data privacy management platform built by a San Francisco-based vendor with offices in the Americas, Europe, and Asia. The TrustArc Platform provides expert consulting and proven methodologies to help organizations handle all phases of privacy program management. It's also the first organization to join the Safe Harbor framework back in 2000.



Founded in 2016, OneTrust supports organizations in showing accountability and compliance with a number of global regulations. With offices in Atlanta, Georgia and in London, England, the young company is quickly gaining recognition as a fast-growing and reliable privacy management technology platform.



Cookiebot is a cookie and online tracking consent solution created by Cybot. The company is based in Copenhagen, Denmark. It delivers automated ePrivacy services that allow website operators to respect and protect the privacy of their visitors.



Consentmanager.net is a Consent Management Provider, a project of Jaohawi AB, headquartered in Västerås, Sweden. Jaohawi AB has over 10 years of experience in the field of ad technology. ConsentManager.net has been used to help newspapers, advertising agencies and networks.

2.4 Data collected in online learning

New technologies—including personal computers, mobile devices, apps, websites, programs, and online learning tools—are used in classrooms in ways that cause new data to be generated about individual students that never existed before including drafts and edits as they are recorded and showing the pacing and record of their performance through a math or reading program. Communications between students and teachers, or students and other students—along with everything from last night’s math homework to the metadata of their online behavior while immersed in an app—is now created, collected, and often held by third party educational technology vendors.

(1) What is metadata?

Metadata is data that helps describe other data. Today, metadata is electronic, but historically, it was contained in a library card catalog. Metadata consists of tags generated by some combination of computers and humans.

On most webpages, metadata consists of tags that help other websites and applications understand what it is about. For example, a website may simply list the address of Beijing Normal University without any metadata might say, “the university is in Beijing over on Xijiekouwai Street.” To make the university easier to be found and read by machines and people, website may translate that data into metadata for location: “Beijing” and “Xinjiekuwai St.”

(2) Metadata in education

As schools ramp up virtual classrooms, encourage students, teachers and parents to use online learning tools, and allow the use of digital applications, privacy need to be front and center. Besides personal data listed on Chapter 2, there is another word “metadata” that we should pay attention to. Online learning tools collect a large amount of contextual or transactional data as part of their operations, often referred to as “metadata.”

Metadata refer to information that provides meaning and context to other data being collected; for example, information about how long a particular student took to perform an online task has more meaning if the user knows the date and time when the student completed the activity, how many attempts the student made, and how long the student’s mouse hovered over an item (potentially indicating indecision).

Metadata has implications beyond privacy. In education, where technology offers the potential to “personalize” the learning experience for students, metadata is critical. The more comprehensive the metadata on a resource, the easier it is for other tools and services to use. Metadata offers enormous potential for online learning resources to be accessible through personalized learning platforms emerging today.

Further Reading

Sharable Content Object Reference Model (SCORM)

Shareable Content Object Reference Model (SCORM) is a collection of standards and specifications for web-based electronic educational technology (also called e-learning). It defines communications between client side content and a host system (called “the run-time environment”), which is commonly supported by a learning management system. SCORM also defines how content may be packaged into a transferable ZIP file called “Package Interchange Format.”

SCORM is a specification of the Advanced Distributed Learning (ADL) Initiative from the Office of the United States Secretary of Defense.

SCORM 2004 introduced a complex idea called sequencing, which is a set of rules that specifies the order in which a learner may experience content objects. In simple terms, they constrain a learner to a fixed set of paths through the training material, permit the learner to “bookmark” their progress when taking breaks, and assure the acceptability of test scores achieved by the learner. The standard uses XML, and it is based on the results of work done by AICC, IMS Global, IEEE, and Ariadne.

2.5 Students and parents' rights to data

Online services collect increasing amounts of personal data about their users and leverage it to extract valuable knowledge about them. This data can be used for providing new services and for profiling individuals, and the results are monetizable input for e.g. targeted advertising. Unfortunately, individuals themselves typically have little or no control over how their data is created or used.

As a digital citizen and an online learner, it's important to understand these rights to ensure you are safe when using the Internet.

(1) Data subject rights

Privacy laws grant people the rights to keep their personal data. Under the GDPR and other privacy protection laws, individuals have certain rights to their personal information. These are:

- The right to access
- The right to be forgotten
- The right to data portability
- The right to be informed
- The right to have information corrected
- The right to restrict processing
- The right to object
- The right to be notified

(2) Students and parents' rights

Students and parents have rights to access personal data that the school or third party such as online learning tools holds about them. Parents can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data or where the child has provided consent. Parents also have the right to make a subject access request with respect to any personal data the school holds about them. If parents make a subject access request, school or online learning tools should:

- Give parents a description of it
- Tell parents why we are holding and processing it, and how long they will keep it for
- Explain where they got it from, if not from parents or children
- Tell parents who it has been, or will be, shared with
- Let parents know whether any automated decision-making is being applied to the data, and any consequences of this
- Give parents a copy of the information in an intelligible form

Further Reading

Measures for the Determination of the Collection and Use of Personal Information by Apps in Violation of Laws and Regulations developed by the Secretary Bureau of the Cyberspace Administration of China

The following acts of an App may be determined as “failing to make public the collection and use rules”

- There is no privacy policy in the App, or there are no rules on collecting and using personal information in the privacy policy.
- Users are not given a prompt through obvious methods such as pop-up windows that they should read the privacy policy and other collection and usage rules when the App runs for the first time.
- It is difficult to access collection and usage rules such as privacy policy. For example, after entering the main interface of the App, a user cannot access collection and usage rules unless he or she clicks the menu button more than four times or conducts other operations.
- It is difficult to read collection and usage rules such as the privacy policy. For example, the characters are too small or too close to each other, too light in color, or blurred, or no simplified Chinese version is provided.

The following acts of an App may be determined as “failing to explicitly show the purposes, methods and scope of the collection and use of personal information

- The purposes, methods and scope, among others, of the collection and use of personal information by Apps (including entrusted or embedded third-party codes and plug-ins) are not listed one by one.
- When the purposes, methods and scope of the collection and use of personal information change, users are not notified in appropriate manners which include but are not limited to updating the privacy policy and other collection and use rules and reminding the users to read such rules.
- When applying for opening the permission to collect personal information, or for collecting personal sensitive information such as a user's ID number, bank account number or whereabouts, the App fails to notify the user of its purpose, or the purpose given is unclear and difficult to understand.
- The content of the relevant collection and usage rules is obscure, verbose, and cumbersome, and is difficult for users to understand. For instance, a lot of terminologies, among others, are used.

The following acts of an App may be determined as “failing to collect and using personal information with a user’s consent”

- The App starts to collect personal information or open the permission to collect personal information before obtaining the user’s consent.
- After the user clearly expresses his or her disagreement, the App still collects personal information or opens the permission to collect personal information, or frequently asks for the user’s consent or interferes with the normal use of the user.
- The personal information actually collected or the permission to collect personal information opened is beyond the scope authorized by the user.
- The user’s consent is sought in a non-explicit manner, such as selection of “agreeing to the privacy policy” by default.
- The authority status concerning whether collection of personal information is permitted as set by the user is changed without the user’s consent. For instance, the App automatically restores the authority status set by the user to the default state when the App is updated.
- The App pushes information in a directional manner by using the user’s personal information and algorithm and does not provide the option of non-directional push of information.
- The user is misled into agreeing to the collection of personal information or opening of the permission to collect personal information by improper methods such as fraud or coaxing, such as deliberately deceiving the user by concealing the true purpose of collection and use of personal information.
- The user is not provided with the channels and methods for withdrawing the consent to collect personal information.
- Personal information is collected and used in violation of collection and use rules declared by the App.

Chapter 3 Preparing Devices, Network, and Tools

Before learning online, preparing the devices, networking, tools, and reading privacy policy are basic aspects for personal data protection, which can guarantee the quality of online learning.

3.1 Setting up your device

Level	Know/Vigilant/Protect yourself/Protect others
Related Users	Students, Parents, Teachers
Related Privacy	Personal data stored in devices such as personally identifiable information
Risks	• Loss or Theft • Abandonment or Switch

To protect the personal data, the first thing is to ensure the digital devices are setting up appropriately, including selecting the devices and keep the devices safe.



Topic: What online learning devices can I choose?

1) Tablets and Smart phones

They are light, mobile, tactile and relatively simple to use for all age groups and are great for writing and drawing, capturing photos and videos, and making sound recordings.

2) Laptops

They have the benefit of an integrated keyboard that tablets lack. Their portability means that they can be used in different environments.

3) Desktops

The full keyboard and larger screen size of desktops are more conducive to extended tasks and to students able to work together around them. They can work with a cabled connection rather than being reliant on Wi-Fi so network-intensive tasks such as transferring large files can be faster.



Topic: How can I keep my device safe?

- Take care of cameras and microphones on devices.
- Keep personal equipment in public places to prevent theft.
- Keep your devices locked and set secure passwords.
- Keep your devices' operating system up-to-date.
- Install anti-virus software.
- Do not jailbreak or root your phone.
- Make regular backups of important personal data.

3.2 Managing network connection on your device

Level	Know/Vigilant/Protect yourself/Protect others
Related Users	Students, Parents, Teachers
Related Privacy	Personal data stored in devices such as personally identifiable information
Risks	• Network Intrusion • Man-in-the-Middle Attack • Browser Hijacking

Network security keeps unauthorized users and hackers from accessing your Wi-Fi network and the devices that use it. It is important to connect and use Internet safely.



Term: Wi-Fi

Wi-Fi is a technology for electric devices to connect to a wireless local area networking (WLAN). Wi-Fi is usually referred to as wireless network.



Topic: How to connect mobile devices to the Internet?

1) 4G Connection

4G-enabled devices connect to the Internet through their providers' cellular connection. Data being sent via 4G are encrypted, making 4G safer than public Wi-Fi.

2) Private Wi-Fi Connection

Private Wi-Fi connections, when properly set up, allows password-protected access and encryption to the data that are being sent and received.

3) Public Wi-Fi Connection

Public Wi-Fi hotspots are found in public places such as airports, coffee shops, hotels, etc. Public Wi-Fi is the least safe way to connect to the Internet, and it's really a wildcard.



Term: Virtual Private Network (VPN)

A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated circuits or with tunneling protocols over existing networks.



Topic: How can I use the Internet safely?

When it comes to public Wi-Fi, there are more opportunities for attackers to exploit vulnerabilities via your connection over Wi-Fi than over 4G. As to the security of these connections, here's how they rank from the most secure to the least secure:

- Using a VPN over a cellular network or using a VPN over Wi-Fi.
- Cellular only.
- Wi-Fi only.

3.3 Selecting and installing learning tools

Level	Know/Vigilant/Protect yourself/Protect others
Related Users	Students, Parents, Teachers
Related Privacy	Personally Identifiable Information, biometric information
Risks	• Fake or Malicious Websites • Computer Viruses • Malicious Software

What should we notice when we select, download and install online learning tools? Here are some relevant suggestions.



Topic: How do I, as a teacher, select tools for my students?

1) Suitability

You may want to consider if the tools serve your instructional purpose.

2) Ease of Use

In deciding whether to select a tool, be sure to evaluate the tool as a non-user. Try to determine how

easy or difficult it will be for your students to achieve a level of competence with the tool such that they can use it to learn effectively and participate meaningfully.

3) Accessibility

Be sure to choose tools that are accessible as outlined by the Universal Design for Learning (UDL) principles of flexible, adaptable curriculum design to support multiple learning approaches and engagement for all students and in terms of legislative requirements for meeting the specific accessibility needs of learners with disabilities.

4) Required Equipment

You may want to survey your students' access to technology when selecting tools. For example, all students may not have access to webcams or microphones which would inhibit their ability to do web-conferencing.



Term: Secure Socket Layer (SSL)

SSL is a security protocol implemented on top of TCP/IP protocols. SSL supports various network and it provides three basic security services, all of which are enabled by a public key and a symmetric key.



Topic: How do I safely download and install software?

Check the Website Address: Websites without SSL/TLS encryption or without the requisite certificates to prove they have utilized that type of security measures cannot guarantee you anything.

Download from canonical sources: Install software from the official websites and the operating systems' own application stores, such as Microsoft Store, Apple App Store, Google Play Store, etc.

Pay attention to the pricing information: See whether you have to pay for upfront signup costs, per-use fees, etc.

3.4 Browsing the privacy policy

Level	Know/Vigilant
Related Users	Students, Parents, Teachers
Related Privacy	Basic information
Risks	Misuse of data by online learning tools

Many privacy laws around the world require businesses to provide their customers with a privacy policy. It typically details important legal information about your data, including what information the app collects, how the company uses it, with whom it shares it, and how it protects it. Learners should not ignore the information, but to read the privacy policy carefully.



Topic: Where to find the privacy policy?

1) Twitter

Privacy Policy URL: <https://twitter.com/en/privacy>

Find on Android: Your Profile Avatar → Settings → My Devices Legal Information → Privacy policy

Find on iOS: Your Profile Avatar → Settings and privacy → About Twitter → Privacy policy

2) YouTube

Privacy Policy URL: https://support.google.com/youtube/answer/7671399?p=privacy_guidelines

Find on Android: Your Profile Avatar → Terms & privacy policy

Find on iOS: Your Profile Avatar → Terms & privacy policy

3) Zoom

Privacy Policy URL: <https://zoom.us/privacy>

Find on Android: Settings → Privacy Policy

Find on iOS: Settings → Privacy Policy

4) IXL

Privacy Policy URL: <https://www.ixl.com/privacypolicy>

Find on Android: Your Profile Avatar à About Us à Privacy policy

Find on iOS: Your Profile Avatar à Settings and privacy à About IXL à Privacy policy

5) Edmodo

Privacy Policy URL: <https://go.edmodo.com/privacy-policy>

Find on Android: Create Free Account à Select Who are you à Privacy policy

Find on iOS: Create Free Account à Select Who are you à Privacy policy

Further Reading



1) Choosing the right digital device

This guide will provide you with information that will help you as you decide which devices to choose for your online learning. It is important to consider not just the devices but how you use them and which device is best for which sorts of activities for effective teaching and learning. It will also be useful for schools providing advice to parents about which type of device to purchase.

Link: <http://elearning.tki.org.nz/Technologies/Technical-support-and-procurement/CLA-resources/Choosing-the-right-digital-device>



2) Instructional technology and digital learning

Data and research about instructional technology are presented in two sections. The first section focuses on the availability or use of various technological devices in classrooms and other topics such as internet access. The second section focuses on online learning, providing data about its prevalence and the different types of on-

line learning available to students. Each section concludes with a review of the research on the effectiveness of the technology discussed and its impact on student learning outcomes.

Link: <https://nsf.gov/statistics/2018/nsb20181/report/sections/elementary-and-secondary-mathematics-and-science-education/instructional-technology-and-digital-learning>



3) How to find great learning resources for your students during school closures?

Whether you're used to teaching with tech or not, transitioning to distance learning is a big undertaking. So many variables will determine your specific needs -- from your students' ages and access to technology, to the goals and expectations your school district has outlined for you. While you're ultimately going to know which tools are best for you and your students, we're here to provide inspiration and support. We have thousands of reviews that dig into the pros, cons, and "how-to" of each app, website, and game. To make sifting through these reviews easier, we've put together this collection of our most relevant Top Picks lists.

Link: <https://www.commonsense.org/education/articles/how-to-find-great-learning-resources-for-your-students-during-school-closures>



4) Remote learning and virtual classroom platforms

The sites provided in the link below allow teachers to follow their existing lesson plans by creating their own online learning resources. Some also provide the platforms they need to host virtual interactive multimedia classrooms.

Link: <https://www..com/free-online-learning-resources/#platforms>



5) Student privacy pledge

The Future of Privacy Forum (FPF) and The Software & Information Industry Association (SIIA) of US introduced a Student Privacy Pledge to safeguard student privacy regarding the collection, maintenance, and use of student personal information. You can find all the privacy policy links of the signed Apps below.

Link: <https://studentprivacypledge.org/signatories/>

Chapter 4 Preserving Privacy when Signing up/in on Learning Platforms

When signing in to any learning platforms, first and foremost, users should register in the platform; however, it is often ignored, and consequently they may forget the username/password, or the password is leaked.

4.1 Using strong passwords to create accounts

Level	Know/Vigilant/Protect yourself
Related Users	Students, Parents, Teachers
Related Privacy	Personally Identifiable Information, network identity information
Risks	• Weak Passwords • Password Leak

Registered users normally provide some sort of credentials (such as a username or e-mail address, and a password) to the system in order to prove their identity. It is of vital importance for users to set strong password, to protect the password leak, and to preserve the biometric information.



Topic: How do I create a strong password?

- It contains at least eight characters or more
- It contains a mix of four different types of characters: upper/lower case letters, numbers and special characters like */'&
- If you only have one special character in your password don't make it the first or last character in your password i.e. aGdQl01@
- It shouldn't be a name or word in any language in the dictionary
- It shouldn't include any part of your name, address or date of birth

- You can keep a hint of your password but don't include any related services or websites linked to it
- Use a different password for every service or website.



Topic: Use password management tools

Password management tools, or password vaults, are a great way to organize your passwords. They store your passwords securely, and many provide a way to back up your passwords and synchronize them across multiple systems. Below we have a list of the best free password managers out there. All of these services offer fantastic features, so if you want to find out more about any of the services below, click the links to the provider's website or scroll below this list for a summary of what makes each service great. (Endorsement not implied)

- Keepass - An excellent free password manager
- Bitwarden - An open-source password manager built to be user-friendly
- Password Safe - Keeping you safe, one password at a time
- LastPass - The free tier doesn't skimp too much from its premium service
- RoboForm - Highly-featured and easy to use

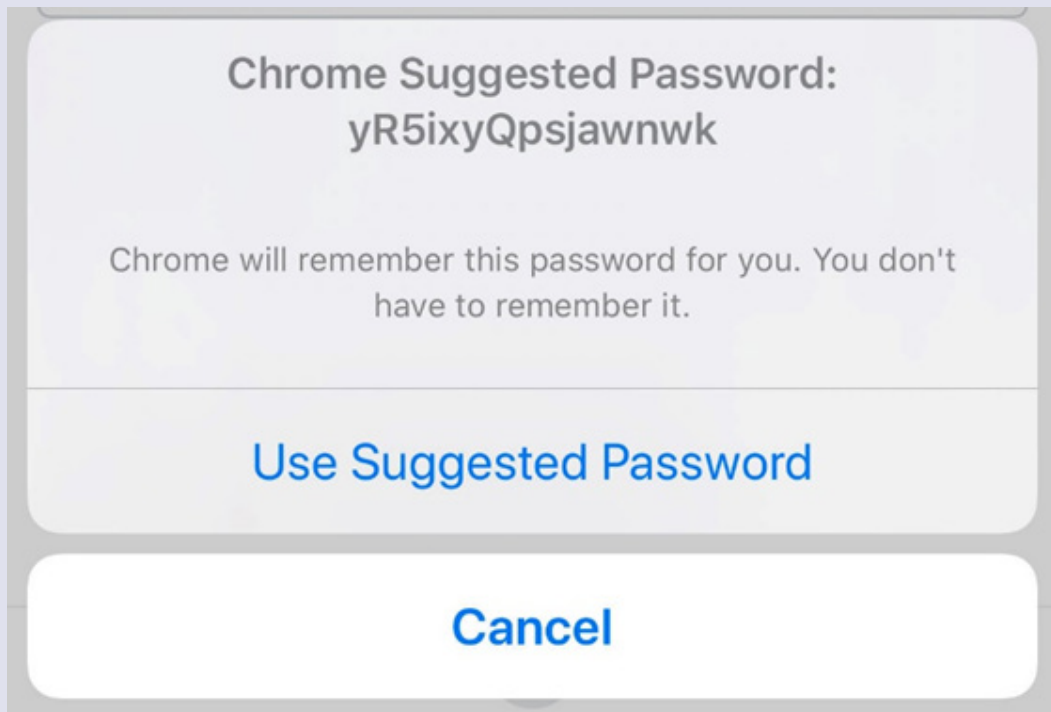


Topic: How to generate strong password with google chrome or iOS?

When you are creating online accounts, there are some rules such as "password must be at least 8 characters", "password must contain at least one upper letter" and so on. You can let google chrome or iPhone create strong passwords for many of your accounts, or you can create your own passwords.

Generate a password with google chrome

To get the latest official operating instructions, visit <https://support.google.com/chrome/answer/7570435?co=GENIE.Platform%3DiOS&hl=en&oco=0>



1) On Android

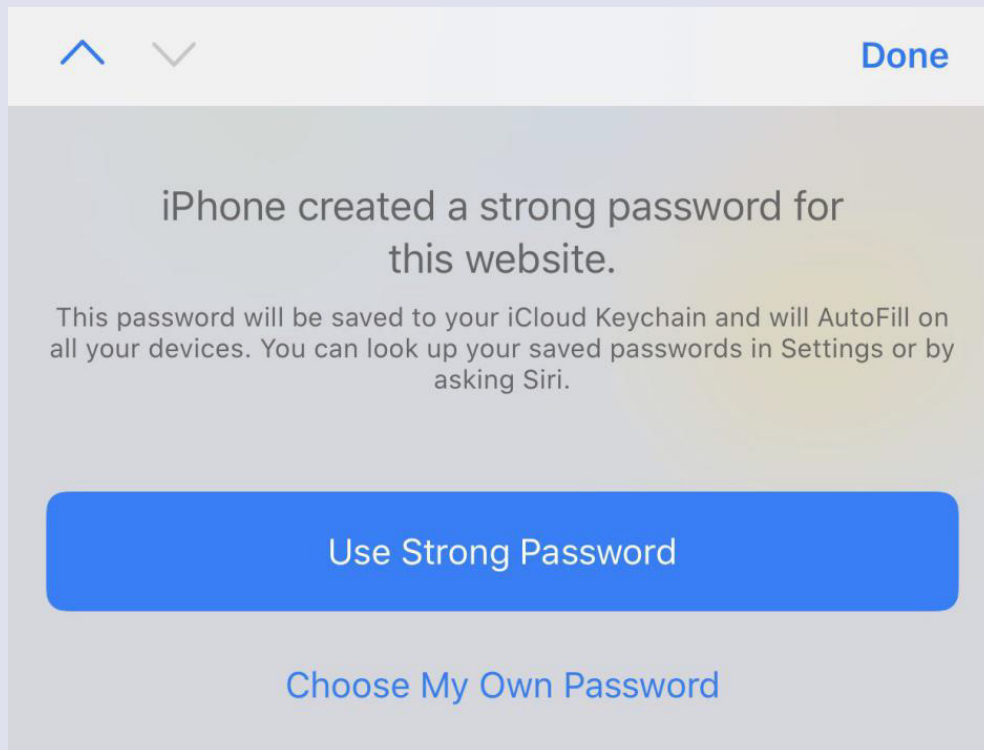
- a) Turn sync on in Chrome.
- b) Go to a website and sign up for an account.
- c) Tap on the password text box.
- d) Tap Suggest strong password.
- e) If you don't see this option, tap Password > Suggest strong password.
- f) You'll see a preview of the password. To confirm, tap Use password.
- g) Finish signing up for your account. Your password is automatically saved to Chrome.

2) On PC

- a) Turn sync on in Chrome.
- b) Go to a website and sign up for an account.
- c) Click the password text box > Suggest Strong Password.
- d) If you don't see this option, right-click the password text box, then click Generate password.
- e) You'll see a preview of the password. To confirm, click Use suggested password.
- f) Finish signing up for your account. Your password is automatically saved to Chrome.

Create website and app passwords on iPhone

To get the latest official operating instructions, visit <https://support.apple.com/guide/iphone/create-website-and-app-passwords-iphf9219d8c9/ios>



- a) On the new account screen for the website or app, enter a new account name.
- b) For supported websites and apps, iPhone suggests a unique, complex password.
- c) Do one of the following:
 - Choose the suggested password: Tap Use Strong Password.
 - Make up your own password: Tap Choose My Own Password.
- d) To later allow iPhone to automatically fill in the password for you, tap Yes when you're asked if you want to save the password.



Term: Uniform Resource Locator (URL)

A Uniform Resource Locator (URL), colloquially termed a web address, is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.



Topic: How do I protect my passwords from leaking?

Don't click on links or attachments in unsolicited messages. It's always better to type an URL directly into your browser to avoid the risk of being taken to a phishing site.

Use two-factor authentication. Increasingly, online providers help you secure your account by requiring you to enter a one-time code as well as your normal password.

Keep a close eye on your different accounts for any suspicious activity, and contact the providers immediately if you see anything at all amiss.

Other safe tips for security:

- a) Don't share passwords between people or systems
- b) Don't do your banking on shared computers or laptops
- c) Take care using your mobile on free Wi-Fi in cafés, banking is not safe
- d) Do not write your password on post-it notes or store it in an unsecured memo on your mobile
- e) Do not keep a list in unprotected documents, text files or spreadsheets on your laptop
- f) Avoid using the same password on multiple websites; you can expose all of your accounts in one go.



Topic: What are biometric identifiers?

Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palmprint, hand geometry, iris recognition, retina and scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics.



Topic: How can I protect my biometric information?

Strong passwords: It's harder to steal your data by simply cracking your password. Keeping your biometric information in only a few, limited places largely prevent hackers from breaching your data.

Keep your software up-to-date: When your device manufacturer notifies you of an available software update or patch, install it right away to help reduce the opportunity of your device being vulnerable to security flaws. It's especially important to keep your operating systems and Internet security softwares up-to-date.

Choose not to give biometric identifiers: If you're worried about the security of your biometric data, sometimes you can opt out of providing it. Consider a smartphone that doesn't require fingerprint authentication or choose not to use facial recognition software. You can also disable facial recognition in your App's settings.

4.2 Signing in a device that's not yours

Level	Know/Vigilant/Protect yourself
Related Users	Students, Parents, Teachers
Related Privacy	Personally Identifiable Information, network identity information
Risks	User Information Leakage

Public computers in libraries, Internet cafes and airports can be safe if you follow a few simple rules when you use them.



Topic: How to use a public computer safely?

1) Don't save your login information

Always log out of websites by clicking "log out" on the site. It's not enough to simply close the browser window or type in another address.

Many programs (especially social networking websites, web-based emails, and instant messaging systems) include automatic login features that will save your username and password. Disable this option so that no one else can log in as you after you have finished using the computer.

2) Don't leave the computer unattended with sensitive information on the screen

If you have to leave the public computer, log out of all programs and close all windows that might display sensitive information.

3) Erase your tracks

Internet Explorer 9 offers InPrivate browsing that leaves no trace of a specific web activity. If you do not choose InPrivate browsing, Internet Explorer keeps a record of your passwords and every page you visit, even after you've closed them and logged out.

4) Disable the feature that stores passwords

Before you start surfing the web, turn off the Internet Explorer feature that 'remembers' your passwords.

- a) In Internet Explorer, click "Tools", and then click "Internet Options".
- b) Click the "Content" tab, and then click "Settings", next to "AutoComplete".
- c) Click to clear both check boxes having to do with passwords.

5) Delete your temporary internet files and browsing history

When you finish using a public computer, you can help protect your private information by deleting your temporary internet files.

6) Watch out for over-the-shoulder snoops

When you use a public computer, look out for thieves who look over your shoulder or stand particularly close to you in order to take note of your sensitive information (such as passwords) as you enter them on the computer.

7) Don't enter sensitive information into a public computer

The above measures provide some protection against casual hackers who use a public computer after you have used it.

But keep in mind that a really industrious thief might have installed sophisticated software on the public computer that records every keystroke and then emails that information back to him.

Then, it doesn't matter if you haven't saved your information or if you've erased your tracks. They still have access to this information.

If you really want to be safe, avoid entering any sensitive information into any public computer, especially your credit card number or any other personal or financial details.

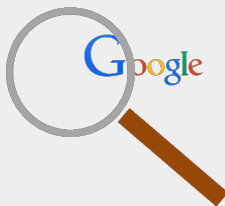
Further Reading



1) ICT security booklet on UNESCO's information systems

Basic concept of information security and general tips for protecting yourself.

Link: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/ERI/pdf/ICTSecurityBooklet_En.pdf



2) Use the privacy checkup feature to boost your google account privacy.

One simple way to boost your Google account privacy is to use the Privacy Checkup feature. In a number of simple steps, the tool enables you to manage your data on various products and services run by the company.

Link: <https://myaccount.google.com/privacycheckup>



3) Two-factor authentication provides security against various attacks.

The second authentication factor might be a minor inconvenience, but it provides a major security boost

Link: <https://www.welivesecurity.com/2019/12/13/2fa-double-down-your-security>



4) Risk of not enabling MFA (also commonly known as two-factor authentication)

More than 99.9 percent of Microsoft enterprise accounts that get invaded by attackers didn't use multi-factor authentication (MFA). This session will describe the dangers and the surprises of Microsoft's journey toward 100 percent remediation with practical guidance to help with yours.

Link: https://youtu.be/B_mhJO2qHIQ



5) Create a strong, long and complex password.

Passwords are often the first line of defense in protecting our personal and financial information. The one-minute guide shows you how to create a strong, long and complex password.

Link: https://youtu.be/q5DYkzOrz_I

Chapter 5 Protecting Privacy when Navigating Learning Platforms

After signing in to a learning platform, learners could enroll in the courses, post messages in forums, blogs, browse and learn the contents. This section will introduce the issues associated with the personal data protection in navigating learning platforms.



Term: Learning management system (LMS)

A learning management system (LMS) is a software application for the administration, documentation, tracking, reporting, automation and delivery of educational courses, training programs, or learning and development programs.

– Ellis, Ryann K. (2009), *Field Guide to Learning Management, ASTD Learning Circuits*, archived from the original on 24 August 2014, retrieved 5 July 2012

Digital learning management systems recommended by UNESCO:

- CenturyTech – Personal learning pathways with micro-lessons to address gaps in knowledge, challenge students and promote long-term memory retention.
- ClassDojo – Connects teachers with students and parents to build classroom communities.
- Edmodo – Tools and resources to manage classrooms and engage students remotely, offering a variety of languages.
- Edraak – Arabic language online education with resources for school learners and teachers.
- EkStep – Open learning platform with a collection of learning resources to support literacy and numeracy.
- Google Classroom – Helps classes connect remotely, communicate and stay-organized.
- Moodle – Community-driven and globally-supported open learning platform.
- Nafham – Arabic language online learning platform hosting educational video lessons that correspond with Egyptian and Syrian curricula.
- Paper Airplanes – Matches individuals with personal tutors for 12-16 week sessions conducted via video conferencing platforms, available in English and Turkish.
- Schoology – Tools to support instruction, learning, grading, collaboration and assessment.

- Seesaw – Enables the creation of collaborative and sharable digital learning portfolios and learning resources.
- Skooler – Tools to turn Microsoft Office software into an education platform.

5.1 Enrolling in an online course

Level	Know/Vigilant/Protect yourself
Related Users	Students, Parents
Related Privacy	Basic information, attendance information, preferred content, study records
Risks	Data leak due to user, site or third parties.

Course enrollment and management are basic functions provided by online learning systems. By enrolling to a course, class or group, it's more convenient and effective for you to manage your study progress and communicate with others.



Topic: How to enroll in a course? (Coursera for example)

1) To enroll in a course

- Open the course information page by clicking on the course title from the Coursera catalog.
- Click Enroll.
- Follow the instructions to enroll in the course. You may have the option for a free trial.

If you want to audit the course instead, look for the Audit option on the course page. Not all courses include this option.

2) See courses you're enrolled in

You can see all the courses you're enrolled in from your Coursera home page. To see all your course

enrollments:

- a) Open coursera.org. Make sure you're logged in.
- b) On the left sidebar, click Enrollments.
- c) Find the "My Courses" section to see courses you're enrolled in.

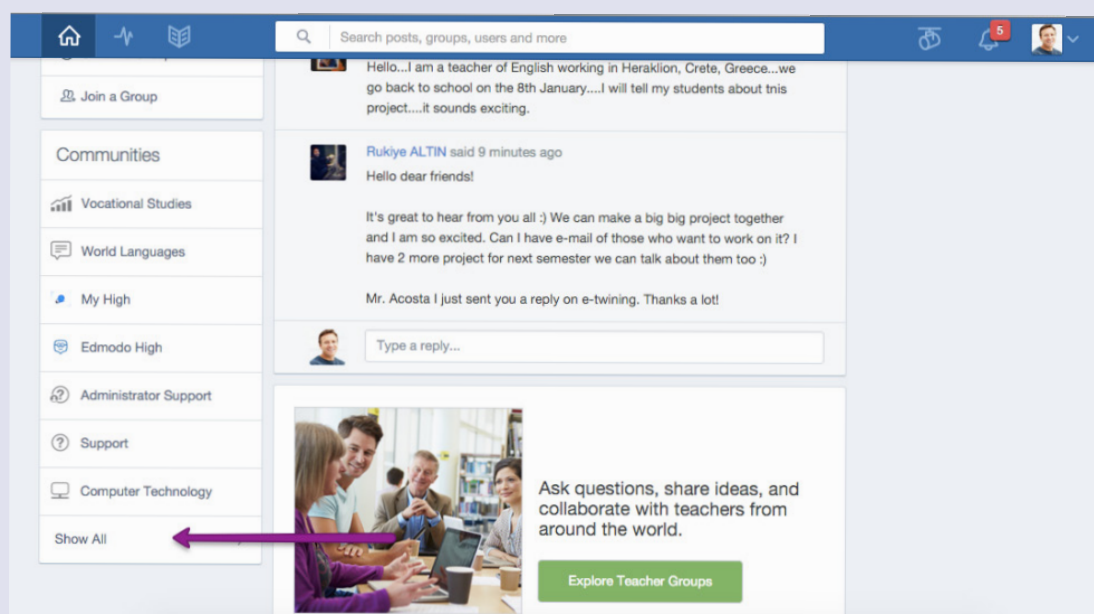
If you enroll in a paid option for any course in a Specialization, you'll see all courses in the Specialization on your Coursera home page, even if you haven't enrolled in or paid for them.

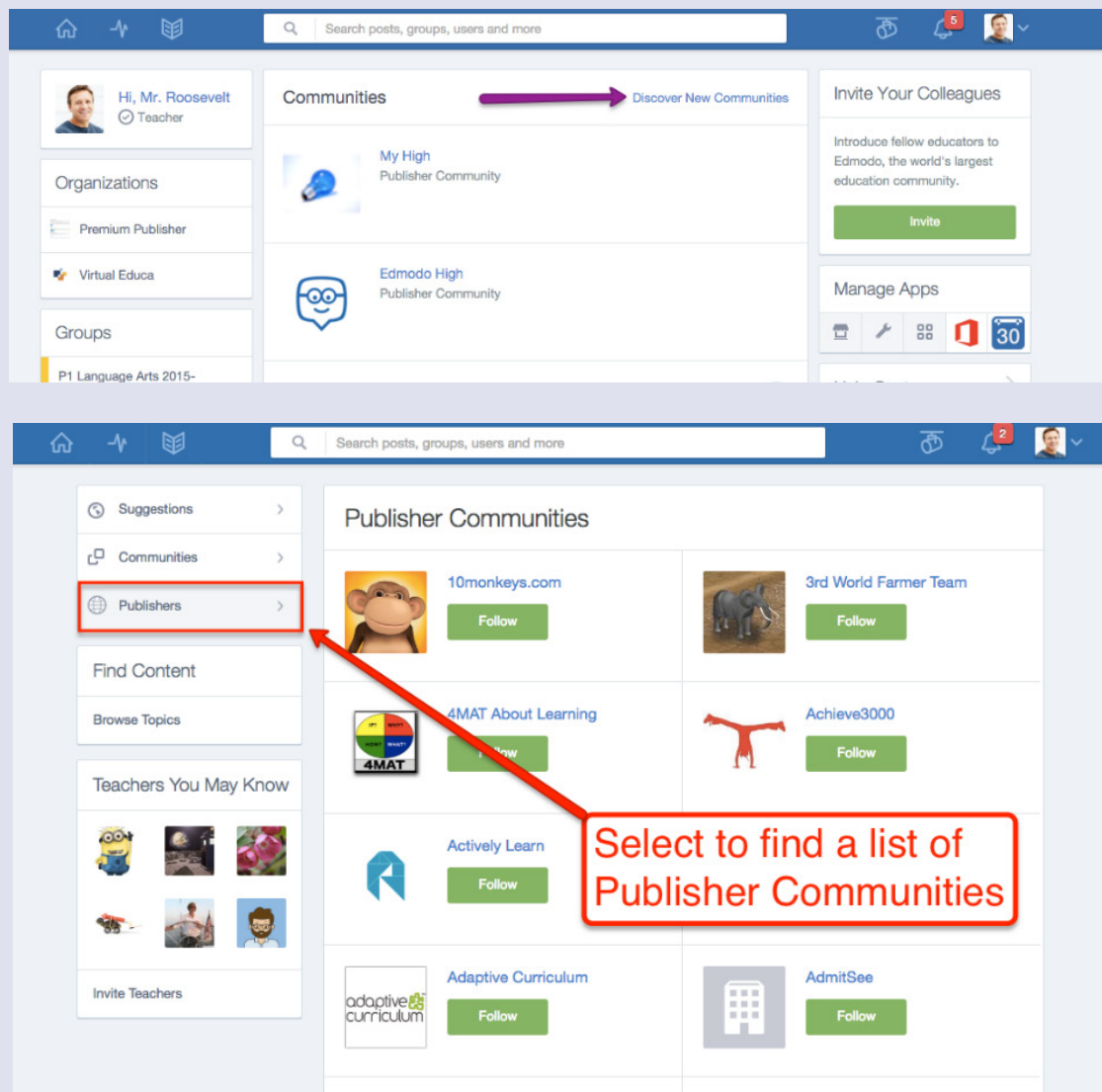


Topic: How to browse and follow communities? (Edmodo for example)

To get started, follow these steps to browse the Communities, then follow those that interest you.

- a) Click "Show All" in the "Communities" section on the left side panel of your Homepage.
- b) Click "Discover New Communities" on the top right to see all communities.
- c) Click on "Follow" directly on this page to follow a Publisher. The button will turn to "Following." Alternatively, you may click the Publisher page to view activity, and then click the green "Follow Publisher" button on the left side panel of the page. The button will turn to "Following."
- d) View Posts from the Community that you are following by clicking "Communities" on the left side panel of your Edmodo page and in your home stream.





5.2 Utilizing personalized learning services

Level	Protect yourself
Related Users	Students
Related Privacy	Personal internet history
Risks	- Extraction and malicious use of information such as user preferences and learning patterns - User information leakage due to outside attack on platforms - Illegal information provision to third-party platforms

Personalized learning is an educational approach that aims to customize learning for each student's strengths, needs, skills and interests. Personalized learning has a lot of potential, but it also has some risks, personal data security is fundamental to any effort to personalize learning.



Topic: What policymakers and education leaders need to know when developing a variety of strategies to personalize learning?

1) Guarantee access to data

Teachers, parents, and students themselves have timely access to the data needed to understand the student's individual needs, set learning goals, and see how the student is progressing toward those goals.

2) Make data use possible

Teachers need training to know how to analyze, protect, and act on data as well as the time to analyze, plan, and collaborate with peers.

3) Protect privacy of student information

This only works if privacy safeguards are in place and everyone using data knows their role in protecting it.

5.3 Using search services carefully

Level	Protect yourself
Related Users	Students
Related Privacy	internet browsing traces
Risks	• Extraction and malicious use of information such as user preferences and learning patterns • User information leakage due to outside attack on platforms • Illegal information provision to third-party platforms

When you study online, you may search in the Internet frequently. However, sometimes searching may put your privacy at risk. You need to pay attention and protect your search privacy.



Term: (Web) Search engine

A search engine is a term commonly used to refer to a web search engine. A web search engine or Internet search engine is a software system that is designed to carry out web search (Internet search), which means to search the World Wide Web in a systematic way for particular information specified in a textual web search query. The search results are generally presented in a line of results, often referred to as search engine results pages (SERPs).



Topic: How to protect your search privacy?

When you learn on the public computer or on other's computer, it is important to remember not to leak your personal information.

1) Don't put personally identifying information in your search terms

Don't search for your name, address, credit card number, social security number, or other personal information. These kinds of searches can create a roadmap that leads right to your doorstep. They could also expose you to identity theft and other privacy invasions.

If you want to do a "vanity search" for your own name, be sure to follow the rest of our tips or do your search on a different computer than the one you usually use for searching.

2) Don't use your ISP's search engine

Because your ISP knows who you are, it will be able to link your identity to your searches. It will also be able to link all your individual search queries into a single search history. So, if you are a Comcast broadband subscriber, for instance, you should avoid using <http://search.comcast.net>. Similarly, if you're an AOL member, do not use <http://search.aol.com> or the search box in AOL's client software.

3) Don't login to your search engine or related tools

Search engines sometimes give you the opportunity to create a personal account and login. In addition, many engines are affiliated with other services – Google with Gmail and Google Chat; MSN with Outlook and Skype and so on. When you log into the search engine or one of those other services, your searches can be linked to each other and to your personal account.

So, if you have accounts with services like Google Gmail or MSN Outlook, do not search through the corresponding search engine (Google or Bing Search, respectively), especially not while logged in.



Term: HTTP cookie

An HTTP cookie (also called web cookie, Internet cookie, browser cookie, or simply cookie) is a small piece of data sent from a website and stored on the user's computer by the user's web browser while the user is browsing.



Topic: How to block “cookies” from your search engine?

From a privacy-protection perspective, it would be best to block all cookies. However, because cookies are necessary for accessing many websites, it may be more convenient (though less privacy-protective) to allow short-lived “session” cookies. These cookies last only as long as your browser is open; therefore, if you quit your browser, re-open it, and then go back to your search engine, your search provider will not be able to connect your current searches with previous ones via your cookies.

Use the following steps to allow only “session cookies,” and remember to quit your browser at least once a day but ideally after each visit to your search provider's site. We recommend that you use Mozilla Firefox and apply these settings:

- a) From the “Edit” menu, select “Preferences”
- b) Click on “Privacy”
- c) Select the “Cookies” tab
- d) Set “Keep Cookies” to “until I close Firefox” 12
- e) Click on “Exceptions,” type in the domains of all of your search sites, and choose “Block” for all of them
- f) Screenshot
- g) If you use Microsoft Internet Explorer to surf the web:
- h) From the Internet Explorer “Tools” menu, select “Internet Options”
- i) Click on the “Privacy” tab and then press the “Advanced” button
- j) Click on “Override automatic cookie handling”
- k) Set both “first party” and “third party” cookies to “Block”
- l) Select “Always allow session cookies”

5.4 Recognizing location services

Level	Know/Vigilant/Protect yourself
Related Users	Students
Related Privacy	Personal location information
Risks	• Threats to personal and property safety caused by location information leakage • User information leakage due to outside attack on platforms • Illegal information provision to third-party platforms

Many applications in your phones/computers require your location information. However, personal information leakage may threaten your property safety or even life safety. You should know how to protect your location information from being stolen.



Term: Location-based service (LBS)

A location-based service (LBS) is a general term denoting software services which utilize geographic data and information to provide services or information to users. LBS can be used in a variety of contexts, such as health, indoor object search, entertainment, work, personal life, etc.



Topic: How to prevent cell phones from being tracked?

- a) Turn off the cellular and Wi-Fi radios on your phone. The easiest way to accomplish this task is to turn on the "Airplane Mode" feature. This shuts down both your cell radios as well as the Wi-Fi radio installed inside your phone so that neither of them can connect to their respective networks.
- b) Disable your GPS radio. Some phones have this as a stand-alone setting, while others

bundle it into menus like Privacy or Location Settings. Turning off location-based features on your phone can prevent your GPS from being activated, which in turn keeps it from providing your phone's location. On some phones, activating "Airplane Mode" will also disable the GPS. Check your phone's user manual for exact instructions.

- c) On Apple's iPhone or iPad: Go into your phone's Settings tab, and then select Privacy. From there, select Location Services. You'll see a string of apps that use location services. You can choose to disable them all by moving the slider at the top, or disable location services only for specific apps. Does Fruit Ninja really need to know where you are in the world? Probably not.
- d) On Android: Open the App Drawer, go into Settings, select Location, and then enter Google Location Settings. Here, you can turn off Location Reporting and Location History. Location Reporting feeds your location data to various apps, while Location History stores your whereabouts for future use in searches and software like Google Now. You can also jettison your entire location history by selecting "Delete Location History" below Location History.
- e) Shut the phone down completely and remove the battery. This is the easiest way to ensure that you can't be tracked via your cell phone, but it comes at the price of not being able to use your phone at all. If you need access to any data on your phone, back it up to a PC before you power down your device.

5.5 Backing up your data

Level	Know/Vigilant/Protect yourself
Related Users	Students, parents, teachers
Related Privacy	Personally Identifiable Information, etc.
Risks	• Reselling of personal information • Advertisements • Life safety

When your computer is attacked by malware, it may cause your files to be lost and damaged, which will affect your learning, working and living. The following are a few ways to back up your system, in case something like that happens.



Topic: How to make a data backup?

Backup of your entire system is your best strategy against hardware failure, software issues (such as from upgrades), and malware that can not only damage an installation but also corrupt your files. If you don't proactively create regular backups, you could end up losing important documents, irreplaceable photos, and custom configurations that you may have spent many hours setting up.

1) Data backup storage solution

A copy of your data is stored in backup storage, and you must have it selected, provisioned, and handy for successful backup (and recovery).

2) Data backup to local or USB disks

If you have enough capacity on your local disks, you can back up to them or to external USB drives. These backups are fast and convenient and you don't need a network. The downside of local backups is that if the system is destroyed by fire or flood, your backups can be destroyed as well if they are stored in the same location. Also in many cases, you need to manage these backups on a computer-by-computer basis, which makes it cumbersome for larger environments.

Local and USB disk backups are best for quick backups of a small number of systems and are designed for the recovery of individual files or systems in the event of software failure.

3) Data backup to cloud storage

The modern alternative to tape backup is cloud storage. With this type of solution, you subscribe to a certain storage capacity in the cloud vendor's or service provider's data center. You do not need any hardware as you do with tape drives, but you do need an internet connection to send backups to the cloud. Your vendor may have ways to eliminate the problems with uploading large amounts of data by offering physical data shipping or initial seeding program.

Further Reading



1) Six ways to use students' smartphones for learning

Smartphones provide an easy way for teachers to “facilitate and inspire student learning and creativity” while increasing motivation, as espoused by the ISTE Educator Standards. Here are six ways to use students' smartphones for learning.

Link: <https://www.iste.org/explore/toolbox/6-ways-use-students-smartphones-learning>



2) Available online courses at free of cost compiled by UNESCO

For continuity of learning, under the overall coordination of Director of UNESCO Nairobi the Science Sector has compiled a variety of educational resources to assist students in Africa continent especially from vulnerable and poor communities.

These educational resources cover many subject areas including natural sciences, mathematics, engineering, arts, social science, etc. to meet the needs of the wider student population.

Link: https://zh.unesco.org/sites/default/files/overview_of_e-learning_materials_0.pdf



3) Useful tools for online learning

The site below shows those best online learning tools for using a blended learning, flipped classroom and distance-learning model respectively for teachers.

Link: https://www.educationworld.com/a_tech/favorite-tools-for-online-learning.shtml

Lifelong Learning



4) Educational websites for lifelong learners

The site below offers a list of websites that have different kinds of educational resources in the fields of history, economy, science and philosophy, include books, videos, audios and courses.

Link: <https://medium.com/@imagnetta/150-educational-websites-for-lifelong-learners-71c1d8e94843>

Chapter 6 Staying Safe while Learning with Social Networking Service

Social networking services are increasingly being used in online learning, providing students with a medium in which they can actively engage with each other and with their teachers, co-create knowledge, share experiences, work and learn collaboratively. However, the use of social network among students may affect their academic life negatively. This is buttressed by the fact that the personal data may leak in social network, their use constitutes distractions, as well as that the students tend to invest a good deal of time in the use of such technologies.



Term: Social network and Social networking service

A social network is a social structure made up of a set of social actors (such as individuals or organizations), sets of dyadic ties, and other social interactions between actors. The social network perspective provides a set of methods for analyzing the structure of whole social entities as well as a variety of theories explaining the patterns observed in these structures.

– Wasserman, Stanley; Faust, Katherine (1994). *“Social Network Analysis in the Social and Behavioral Sciences”*. *Social Network Analysis: Methods and Applications*. Cambridge University Press. pp. 1–27. ISBN 9780521387071.

A social networking service (also social networking site or social media) is an online platform which people use to build social networks or social relationships with other people who share similar personal or career interests, activities, backgrounds or real-life connections.

Collaboration platforms that support live-video communication recommended by UNESCO:

- Dingtalk – Communication platform that supports video conferencing, task and calendar management, attendance tracking and instant messaging.
- Lark – Collaboration suite of interconnected tools, including chat, calendar, creation and cloud storage, in Japanese, Korean, Italian and English

- Hangouts Meet – Video calls integrated with other Google's G-Suite tools.
- Teams – Chat, meet, call and collaboration features integrated with Microsoft Office software.
- Skype – Video and audio calls with talk, chat and collaboration features.
- WeChat Work – Messaging, content sharing and video/audio-conferencing tool with the possibility of including max. 300 participants, available in English and Chinese.
- WhatsApp – Video and audio calls, messaging and content sharing mobile application.
- Zoom – Cloud platform for video and audio conferencing, collaboration, chat and webinars.



Topic: What should I consider in social network?

Whether you are using a networking site, internet dating site or just chatting on a message board, chances are you are putting personal information online. Once it's out there, you may not be able to control what happens to it. This could pose a risk to your privacy or even make you vulnerable to identity theft or fraud

Avoid sharing too many personal details with large numbers of people, for example by allowing open access to your social media pages. Familiarize yourself with the privacy settings of your favorite social networks and adjust them according to your comfort level.

When posting information online it's also worth thinking about who might see it apart from your intended audience—would the things you write or the pictures you post cause embarrassment in real life? How would you feel if your current or potential employer saw what you posted?



Topic: How to use social networking services as learning tools?

It's no secret that our students spend most of their free time on social media websites. Teachers keep seeing their students with their phones, and we usually get frustrated by that habit. It's time to start seeing things differently: Social media can be a useful tool to use for educational purposes.

We'll show you 5 tricks that will reveal the new face of education thanks to Facebook, twitter, and other platforms you can use.

1) Create a Facebook group for your class

- Share something that will make your students laugh.

- Post notes to remind your students about the instructions of important assignments, as well as the submission deadlines.
- Encourage your students to post links to great online resources related to the curriculum. You can give extra points for this activity.
- Constantly search for new online resources that make learning fun, and share the links in the group. Then, ask your students to watch/read/listen to those materials and share their opinions during class.

2) Use blogging for students' homework assignments

How about using blogging as a tool for homework assignment submission? Each student can have a personal blog where they will share book reviews, history research papers, and other assignments they usually submit in print. This is a much better option, since everyone will be able to see what the others have done with the topic, so the healthy competitive spirit will drive them forward.

When you assign team projects, you can ask several “bloggers” to collaborate within a group and publish different parts of the finished paper on each blog.

3) Use twitter for bringing fun into the class

Most educators interested in introducing social media into the teaching processes are focused on Facebook. They perceive Twitter as a network that's mostly used for fun. The fun aspect of Twitter is not necessarily a bad thing.

You can introduce a daily hashtag related to a certain topic you elaborated in class, and ask each student to discover a fun fact related to it. Then, they should post a tweet under that hashtag, and the entire class will follow the activity. This is a great way for the students to realize how the things they learn at school are being implemented in the real world. For example, you can set #spiders for a daily hashtag and start posting fun facts like no 2 #spider webs are the same. Then, ask your students to dig through online resources and discover their own fun facts about spiders. You can all discuss the information you find the next day in class.

4) Use Pinterest for pinning educational resources

You know how hard it is to keep all important online content in the browser's bookmarks. You keep losing the resources you need no matter how hard you try to organize the toolbar. Pinterest is a great platform for organizing educational resources. When you browse and locate something you could use – you just pin it in a board you created for the relevant category.

You can also use Pinterest as a search engine for educational content. Just write your topic in the search bar and you'll discover some cool resources you can present in the classroom.

5) Use YouTube for the flipped classroom concept

This video sharing platform is a great option for introducing the flipped classroom concept into your teaching methods. You can share educational lectures and resources in video format, and expect your students to watch the material instead of writing homework. Then, you can discuss the lecture and do the homework in class.

This concept requires more work on your part, since you'll have to record the lessons and edit the videos. However, you can substitute that effort by telling your students to view free educational videos that have been published by popular YouTubers.

6.1 Using video conference tools with caution

Level	Know/Vigilant/Protect yourself/Protect others
Related Users	Students, Parents, Teachers
Related Privacy	Personally Identifiable Information, personal property information, personal location information
Risks	• Live pictures containing personal identifiable information, personal location information, personal property information, etc. • User information leakage due to outside attack on platforms • User information leakage due to outside attack on personal devices

Webinar by using video conferencing tools is gradually becoming an important method for academic communication and learning in the internet era. It is suggested to use these software safely by considering the following advises.



Topic: Staying safe online whilst livestreaming - advice for parents and carers

1) Talk regularly with your children

Talk regularly with your children about how they use technology and find out what their digital life is like, including what services they are using.

2) Before you stream, protect your personal information.

Make sure your children understand the risks of livestreaming. Live broadcasts can't be edited, and you can't erase what people have already seen. Remind them that personal information might be given away by things said during the stream, things shown on camera or even in the background. Importantly, live-streams can be recorded by others, who can then keep a copy even after the stream has ended or expired.

3) Make an agreement about device usage

Live video can be faked, so encourage your child to think carefully why an unknown person might want to video chat with them. If a site has privacy settings, always make sure your children use them to control who can contact them.

Parents can make a family agreement, where the whole family can be involved in making promises about whether to use streaming services at all, who to use them with, or where in the house it is OK to use them. Parents may decide that devices that can be used for livestreaming and video chatting (such as tablets, phones, webcams connected to computers and laptops) should not be located in bedrooms or more private areas of a house.

4) Teach your child when to say no

Children may be groomed or coerced into appearing naked on camera or performing suggestive acts over webcams. This content can be also recorded and used to threaten or blackmail young people. It's therefore crucial for parents and carers to be aware of children's use of technology and to educate them on the dangers posed to them by offenders.

Tell your child that if he or she is ever asked to say or do something online they don't feel comfortable with, they can always say no, end the chat or broadcast, and talk in confidence with you or another trusted adult. Remind them that it is never too late to tell you about something which has happened online.

5) Report abusive content

Show your children how they can report offensive or abusive material on the service they use to watch livestreams. You can find more information about how you can help your child stay safe online by using features such as privacy settings on social media and understanding how to make a report on a range of apps, games and services.

If you, or your children, ever stumble across child sexual abuse material online, you can also report it to the Internet Watch Foundation. Reporting takes less than 2 minutes and can be done completely anonymously.

6.2 Posting in forums responsibly

Level	Know/Vigilant/Protect yourself/Protect others
Related Users	Students, Parents, Teachers
Related Privacy	Personally Identifiable Information, personal property information, personal information location
Risks	• Extraction and malicious use of information such as user preferences • User information leakage due to outside attack on platforms • Illegal information provision to third-party platforms

You can post something like text, a photo, a video, or a link to an online website. Once posted, it is beyond your control at some degree, so be careful posting online.



Topic: Social network etiquette: How to mind your manners online?

1) What's OK to share?

Posting embarrassing, revealing or negative photos of yourself should be avoided at all costs. Remember: Images you share may be taken at face value, and/or viewed as representative of your character – not to mention live on forever on the Internet. What seems cute in high school or college may not seem quite so endearing to potential employers.

Never share intimate personal details including birthdates, phone numbers, addresses, schools or hometowns online, to minimize risks of crime, vandalism or identity theft. Never let others know when you'll be away from your home, especially for any given length of time, e.g. while on vacation.

Avoid posting on social networks unless you have a tight grasp over your privacy settings and are completely comfortable with the group of online friends that your updates will be shared with.

2) Tone of voice and attitude

Professionalism is imperative – if you wouldn't say it in a social or work setting, don't say it online, in the most public of forums.

Politeness and respect are vital: Always be considerate of others, and treat them the way that you'd wish to be treated.

Poor spelling, punctuation, grammar and choice of words can reflect equally poorly upon the individual – proofread all communications before sending. Shorthand, abbreviations and online slang should be avoided if possible, and used only in the most informal of conversations.

3) Being a responsible user

Understand that various online forums (social networks, blogs, digital communities) have their own rules of conduct, social norms and methods of interaction. Before utilizing one, take a moment to step back and observe how interactions take place, so you can discern appropriate rules of posting, sharing and behavior.

Before posting on others' profiles or walls, or tagging them in your own posts, consider how your actions and/or statements may be perceived.

Use privacy settings to limit who can view your posts and shares.

When asking someone you don't know to be your friend, send a short message explaining who you are and why you're attempting to contact them.

6.3 Surfing the Internet safely

Level	Know/Vigilant/Protect yourself
Related Users	Students
Related Privacy	Personal internet history
Risks	• Extraction and malicious use of information such as user preferences • User information leakage due to outside attack on platforms • Illegal information provision to third-party platforms

Before diving into a course, it's benefits for students to browse around to find something they're interest in. During this stage, it's crucial to make sure the content is appropriate.



Topic: How to block inappropriate content?

1) On windows 10

To get the latest official operating instructions, visit <https://support.microsoft.com/en-us/help/12413/microsoft-account-what-is-family-group>

- a) Open the Start menu. To do so, either click the Windows logo in the bottom-left corner of the screen or press the Win key on your computer's keyboard.
- b) Click the settings gear. You'll see this icon near the bottom-left corner of the Start menu.
- c) Click "Family & other users". This tab is on the left side of the Settings page.
- d) Click the "Manage family settings online" link. You'll see this option below a restricted user's name on this page.
- e) Click Web browsing. This link is to the right of a restricted account's name and profile image.
- f) Click the "Block inappropriate websites" switch. It's below the "Web browsing" heading near the top of the page. Doing so will prevent the restricted account from accessing adult websites on Microsoft Edge and Internet Explorer, as well as on any connected devices (e.g., Xbox One).

2) On mac

To get the latest official operating instructions, visit <https://support.apple.com/guide/mac-help/welcome/mac>

- a) Click the Apple menu. It's the apple-shaped icon in the top-left corner of the screen.
- b) Click "System Preferences". This option is near the top of the drop-down menu.
- c) Click "Parental Controls". It's a yellow icon with a graphic of an adult and a child.
- d) Click the lock icon. It's in the bottom-left corner of the window.
- e) Enter your administrator password. This is the password you use to log into your Mac.
- f) Click "OK". Doing so will unlock the parental controls app.
- g) Click a user's name. Usernames are in the left-hand pane of this window. This should be a user for whom you wish to restrict browsing.
- h) Click the "Web" tab. It's at the top of the window.
- i) Click the "Try to limit access to adult websites" circle. It's near the top of the window. This option will prevent blatant adult content from appearing in Safari.
- j) Click the lock icon again. Doing so will save your changes.

3) On iPhone

To get the latest official operating instructions, visit <https://support.apple.com/en-us/HT201304>
<https://support.apple.com/guide/iphone/welcome/ios>

- a) Open your iPhone's or iPad's Settings. It's a grey app with gears which you'll likely find on the Home Screen.
- b) Scroll down and tap "General". It has a picture of a gear to its left.
- c) Scroll down and tap "Restrictions". If Restrictions are already enabled on your iPhone or iPad, you'll be prompted to enter a passcode. (If you haven't enabled Restrictions, tap Enable Restrictions and create a passcode, then skip the next step.
- d) Enter your Restrictions passcode. This passcode may be different than the passcode with which you lock your iPhone or iPad.
- e) Scroll down and tap "Websites". It's in the "ALLOWED CONTENT" group of options just below the groups of switches on this page.
- f) Tap "Limit Adult Content". This option is near the top of the page. When you tap it, you should see a blue checkmark appear to the right of it.
- g) Tap the "Back" button. It's in the top-left corner of the screen. Doing so will save your settings and prevent the phone's owner from viewing adult sites on the Safari browser. (Consider also sliding the Installing Apps switch left to the "Off" position. This option will prevent other users from downloading different browsers in which to view adult sites.)

4) On Android

To get the latest official operating instructions, visit <https://support.google.com/googleplay/answer/1075738?hl=en>

- a) Open your Android's Google Play Store. It's a white app with a multicolored triangle on it.
- b) Tap . It's in the top-left corner of the screen.
- c) Tap "Settings". This option is near the bottom of the pop-out menu.
- d) Tap "Parental controls". It's near the top of the Settings page.
- e) Slide "Parental controls" right to the "On" position. This option is at the top of the page. It will turn green, signifying that you've enabled parental controls for the Google Play Store.
- f) Enter a four-digit PIN and tap "OK". This will create a PIN for the parental control settings so that they cannot be modified without verification.
- g) Tap a parental control option.
- h) Tap a rating below "18A" on the rating slider. This vertical slider has options from G (most restrictive) up to Allow all. You'll want to tap G, PG, or 14A.
- i) Tap "Save". This will save your content settings.
- j) Tap the "Back" arrow. It's in the top-left corner of the screen.
- k) Repeat this process for each content category. Doing this will prevent your device from

being able to access and download inappropriate content.

- l) Open Google Chrome. It's a red, yellow, green, and blue circular app.
- m) Tap . You'll see this icon in the top-right corner of the screen.
- n) Tap "Settings". This option is near the bottom of the menu.
- o) Tap "Privacy". It's just beneath the "Advanced" tab.
- p) Tap "Safe browsing". This will enable safe browsing on Google Chrome, which means that your Android will no longer display adult sites or other "unsafe" pages.

5) On google chrome

To get the latest official operating instructions, visit <https://support.google.com/families/answer/7087030?hl=en>

- a) Open the Family Link app.
- b) Select your child.
- c) On the "Settings" card, tap Manage settings > Filters on Google Chrome > Manage sites > Approved or Blocked.
- d) In the bottom right corner, tap Add an exception.
- e) Add a website (like www.google.com) or domain (like google). If adding a website, you should include the [www.](http://www) portion of the URL (like www.google.com instead of google.com).
- f) In the top left, tap Close.



Term: Domain Name System (DNS)

The Domain Name System (DNS) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities.

Use secure DNS

When a user requests to visit a web application like facebook.com, the user's computer needs to know what server to connect to so that it can load the application. Computers don't initially have the necessary information to do this "name to address" translation, so they ask a specialized server to do it for them. This specialized server is called a DNS recursive resolver. Some DNS resolvers can block malware and adult contents

- a) Click  on the upper right corner of chrome
- b) Click "Settings"
- c) On Search settings bar, type "dns"
- d) Click "More"
- e) Find "Use secure DNS", click "With CleanBrowsing (Family Filter) or Cloudflare (1.1.1.1)" or "With Custom", here are some DNS address you can use for your family.

Malware Blocking Only

- Primary DNS: 1.1.1.2
- Secondary DNS: 1.0.0.2

Malware and Adult Content

- Primary DNS: 1.1.1.3
- Secondary DNS: 1.0.0.3

For IPv6 use:

Malware Blocking Only

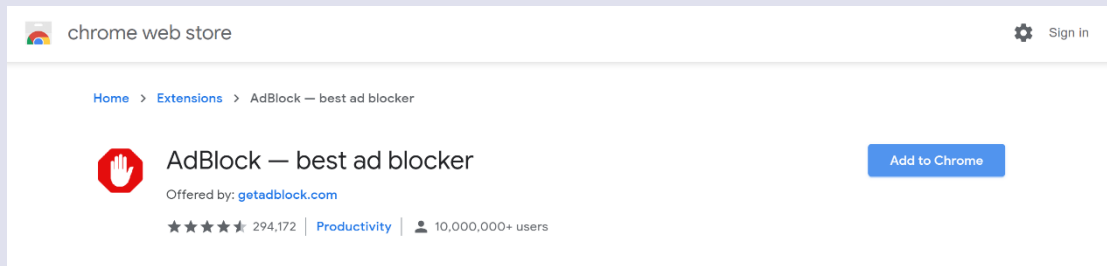
- Primary DNS: 2606:4700:4700::1112
- Secondary DNS: 2606:4700:4700::1002

Malware and Adult Content

- Primary DNS: 2606:4700:4700::1113
- Secondary DNS: 2606:4700:4700::1003

Install ADBlock plugin

- a) Access <https://chrome.google.com/webstore/detail/adblock-%E2%80%94-best-ad-blocker/gighmmpioibklfepjocnamgkkgbiglidom> via google chrome.
- b) Click “Add to Chrome” on the right.



Topic: How to manage your push notifications?

Instant access to important and relevant data is one of the things that makes smartphones so prevalent and clutch in our lives. But when that data is personal, you don't want it showing up on your lock screen for anyone to peer over and see. What's more, push notifications could be disruptive. Notifications might come at inconvenient or downright annoying times. Or they might offer irrelevant information and feel impersonal to the user.

Here are some tip from iPhone User Guide and Android User Guide.

On iPhone with iOS 13

1) Change notification settings

Most notification settings can be customized for each app. You can turn app notifications on or off, have notifications play a sound, choose how and where you want app notifications to appear when your device is unlocked, and more.

- a) Go to Settings > Notifications.
- b) To choose when you want most notification previews to appear, tap Show Previews, then select an option—Always, When Unlocked, or Never. (You can override this setting for individual apps.)

Previews can include things like text (from Messages and Mail) and invitation details (from Calendar).

- c) Tap Back, tap an app below Notification Style, then turn Allow Notifications on or off.
 - If you turn on Allow Notifications, choose how and where you want the notifications to appear for the app—for example, on the Lock screen or in Notification Center.
 - You can also set a notification banner style, sound, and badges for many apps.
- d) Tap Notification Grouping, then choose how you want the notifications grouped:
 - By App: All the notifications from the app are grouped together.
 - Automatic: The notifications from the app are grouped according to organizing criteria within the app, such as by topic or thread.
 - Off: Turn off grouping.

To turn off notifications selectively for apps, go to Settings > Notifications > Siri Suggestions, then turn off any app.

2) Show recent notifications on the Lock screen

You can allow access to Notification Center on the Lock screen.

- a) Go to Settings > Face ID & Passcode (on an iPhone with Face ID) or Touch ID & Passcode (on other iPhone models).
- b) Enter your passcode.
- c) Turn on Notification Center (below Allow Access When Locked).

3) Silence all your notifications

You can also go to Settings > Do Not Disturb, then turn on Do Not Disturb.

On Android

1) Change notifications for your phone

Important: Settings can vary by phone. For more info, contact your device manufacturer.

- a) Open your phone's Settings app.
- b) Tap Apps & notifications > Notifications.
- c) Pick the options you want as your phone's defaults:
 - On lock screen.
 - Allow notification dots.
 - Default notification sound.
 - Swipe fingerprint for notifications.
 - Do Not Disturb.

2) Don't show any notifications

Important: Settings can vary by phone. For more info, contact your device manufacturer.

- a) Open your phone's Settings app.
- b) Tap Apps & notifications > Notifications.
- c) Under "Lock screen," tap Notifications on lock screen or on lock screen.
- d) Choose Don't show notifications.

3) Hide sensitive content from notifications on your lock screen

Important: Settings can vary by phone. For more info, contact your device manufacturer.

- a) Open your phone's Settings app.
- b) Tap App & notifications > Notifications.
- c) Under "Lock screen," turn off Sensitive notifications.



Topic: Deal with online bullying

It is important to remind ourselves that behind every username and avatar there is a real person with real feelings, and we should treat them as we would want to be treated. When bullying or other mean behavior happens, most of the time there are four types of people involved.

- There is the aggressor, or person(s) doing the bullying.
- There is also someone being bullied – the target.
- There are witnesses to what’s going on, usually called bystanders.
- There are witnesses to what’s going on who try to positively intervene, often called upstanders.

If you find yourself the target of bullying or other bad behavior online, here are some things you can do:

If I'm the target, I can

- Not respond
- Block the person
- Report them – tell my parent, teacher, sibling, or someone else I trust, and use the reporting tools in the app or service to report the harassing post, comment, or photo

If you find yourself a bystander when harassment or bullying happens, you have the power to intervene and report cruel behavior. Sometimes bystanders don’t try to stop the bullying or help the target, but when they do, they’re being an upstander. You can choose to be an upstander by deciding not to support mean behavior and standing up for kindness and positivity. A little positivity can go a long way online. It can keep negativity from spreading and turning into cruelty and harm.

If I'm the bystander, I can be an upstander by

- Finding a way to be kind to or support the person being targeted
- Calling out the mean behavior in a comment or reply (remember to call out the behavior, not the person), if you feel comfortable with that and think it’s safe to do so
- Deciding not to help the aggressor by spreading the bullying or making it worse by sharing the mean post or comment online
- Getting a bunch of friends to create a “pile-on of kindness” – post lots of kind comments about the person being targeted (but nothing mean about the aggressor, because you’re setting an example, not retaliating)
- Reporting the harassment. Tell someone who can help, like a parent, teacher, or school counselor.

Further Reading



1) UNICEF For Every Child initiative program

UNICEF works to break that cycle by tackling inequities in opportunity for children who have been marginalized. ... It examines seven sectors that are critical to progress for children: health; HIV and AIDS; water, sanitation and hygiene; nutrition; education; child protection; and social inclusion.

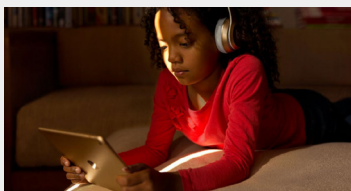
Link: <https://www.unicef.org/>



2) Google safety center for families

Google was founded on the belief that everything we do should always respect the user. As the Internet evolves, this means continuously advancing our security technologies and privacy tools to help keep you and your family safe online. Children today are growing up with technology, not growing into it like previous generations. So we're working directly with experts and educators to help you set boundaries and use technology in a way that's right for your family.

Link: <https://safety.google/families/>



3) Apple families

Apple launched a new Families page that may help give moms and dads the information they need to lock down the iOS and macOS devices their kids are using. In response to growing concern about the effect of its smartphones on children, Apple recently pointed out that it already offers a number of tools to help parents control and restrict the apps, movies, websites, songs, books, cellular data, password settings, and other features on their kids' devices. Now, the Cupertino tech giant is making more of an effort to educate parents about these tools and how to use them.

Link: <https://www.apple.com/families/>



4) Protecting kids online

The Federal Trade Commission (FTC) is an independent agency of the United States government, on its website resources on protecting kids online. The subjects contents Talk to your kids, Kids' online safety and Parental control & rights.

Link: <https://www.consumer.ftc.gov/articles/0031-protecting-your-childs-privacy-online>



5) Center for Internet security

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation.

Link: <https://www.cisecurity.org>

Chapter 7 Clearing Personal Data after Learning Online

After finishing online learning in period, the user should notice the data generated as discussed in the previous chapters, and make the decision on whether to delete the data or not. If you decide to delete the data, the following section provide some suggestions and methods.

7.1 Removing data traces in online learning

Level	Know/Vigilant/Protect yourself
Related Users	Students
Related Privacy	Personally Identifiable Information, personal internet history
Risks	• The platform did not give permission to delete • Illegal retention of information after deleting

When you feel that some content no longer wants to be shared, you can choose to delete them, as long as you have the relevant permissions. Here are some ways to delete content on the typical platform.

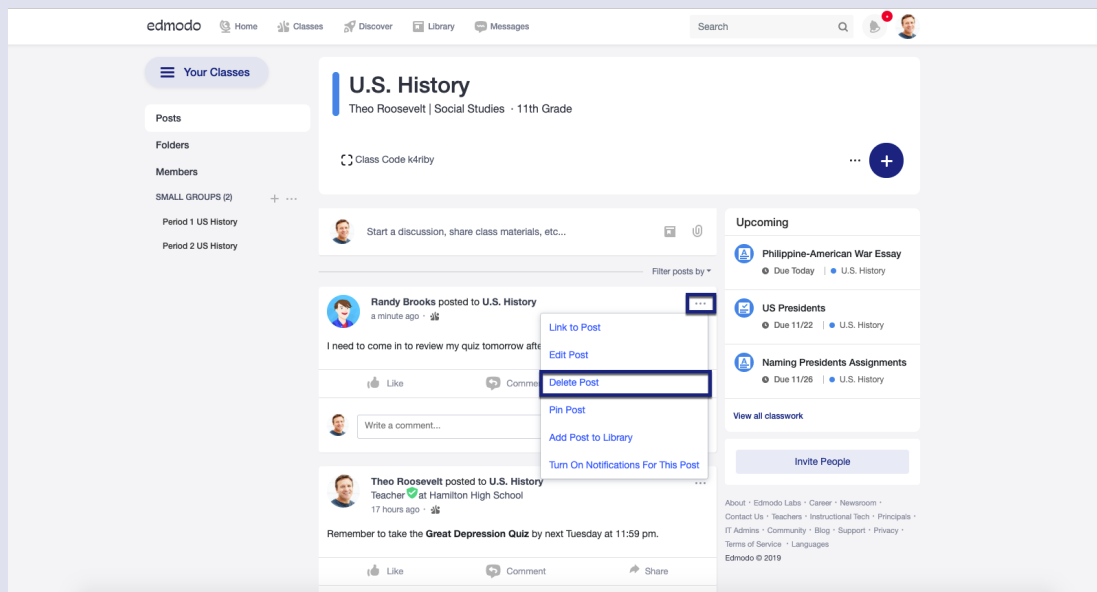


Topic: How to delete user-generated content?

1) Online learning platform – Edmodo

If you are a student, you can delete a post by following these steps:

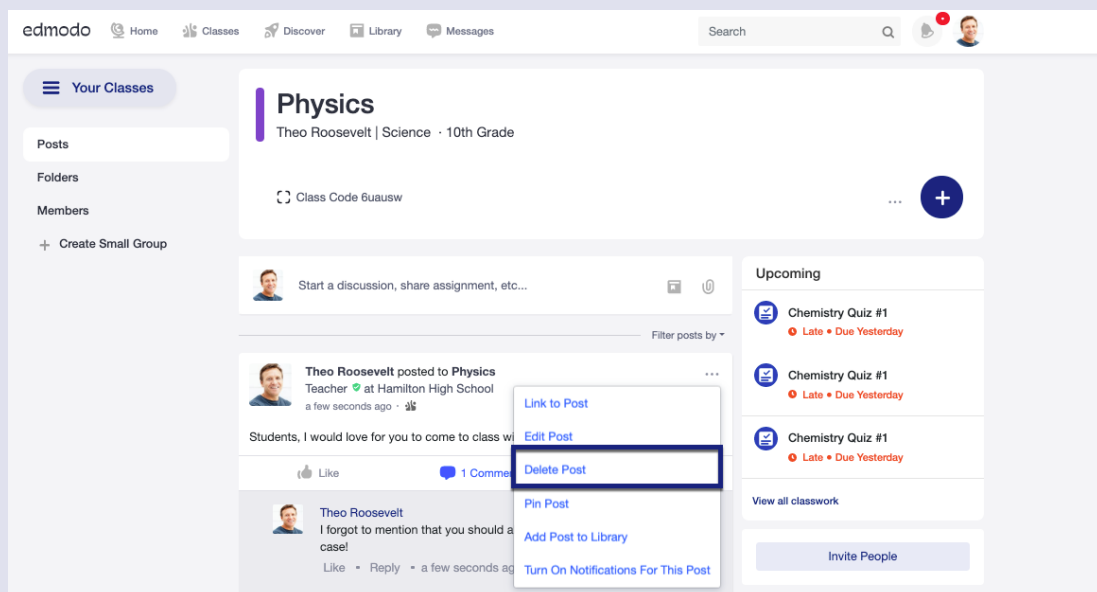
- a) Hover over the post or reply and click the “Post Settings” icon that appears in the top right corner of the post.
- b) Click “Delete Post” or “Delete Reply.”
- c) Click “OK” to confirm.



If you are a teacher, you can delete a post or a comment on a post by following these steps:

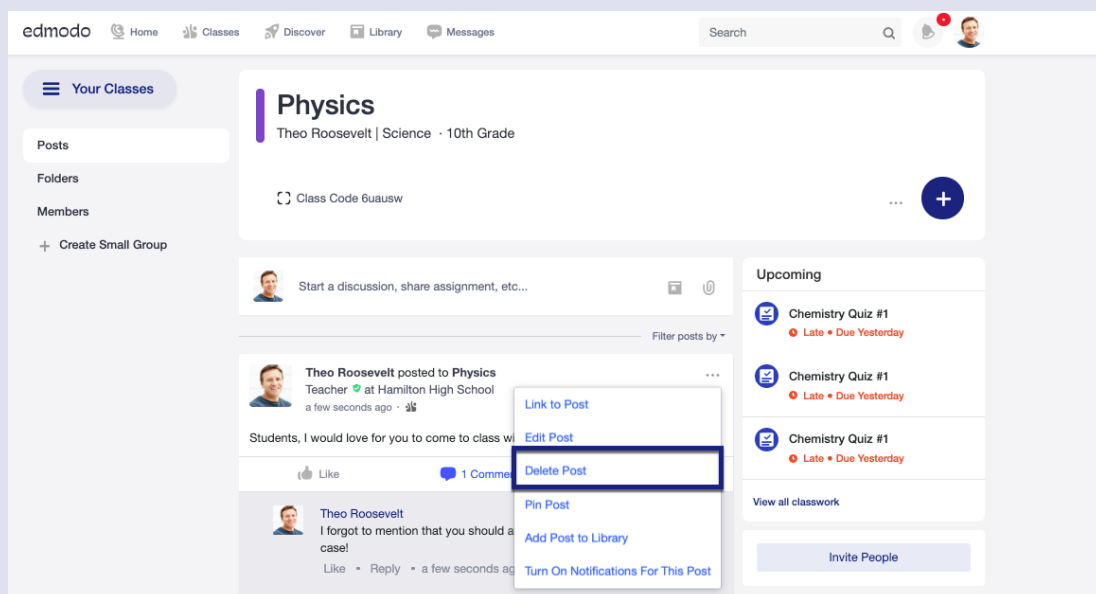
To delete a post:

- Locate the post that you would like to delete
- Click the more button ellipsis.png just to the right of the post to open the popup menu
- Select Delete Post
- Click Delete to confirm



To delete a comment on a post:

- a) Locate the comment that you would like to delete
- b) Click the downward arrow down.png just to the right of the comment to open the popup menu
- c) Select Delete Comment
- d) Click Delete to confirm



2) Online learning platform – Coursera

If you want to leave your organization's learning program:

When you're invited to join a Coursera learning program through a company or organization, you'll get an invitation you'll be able to decline or accept.

If you're already in a Coursera learning program and want to unenroll or be removed from the program, talk to your organization's Coursera for Business admin.

If you want to delete comments or threads in community:

The members cannot delete their threads/posts themselves. You could ask the Community Managers to do that.

3) Social networking – twitter

You can delete your tweet by following these steps:

- a) In the top menu, tap your profile icon.
- b) Tap Profile.
- c) Locate the Tweet you want to delete.
- d) Tap the icon located at the top of the Tweet.
- e) Tap Delete Tweet.
- f) Tap Delete to confirm.

7.2 Deactivating your account

Level	Know/Vigilant/Protect yourself
Related Users	Students
Related Privacy	Personally Identifiable Information, personal internet history
Risks	• The platform does not permit to deactivate • Illegal retention of information after deactivating

When you no longer want to study or have other social activities on the platform, you can choose to deactivate and delete the account, here are some typical platform logout methods for your reference.



Topic: How to deactivate an account?

1) Online learning platform – Edmodo

You can deactivate your own account by following these steps:

- a) Click on the Account icon next to your profile image and then Settings.
- b) Scroll to the bottom of the page and click Deactivate your account.
- c) Read the warning and click Deactivate.

edmodo Home Classes Planner Backpack Discover Messages Search

Save Profile Url

Account

Username
hbenton1218

First Name
Harley

Last Name
Benton

Primary Email
Confirmed

Country:
select

Timezone
select

Save Changes

1. Profile

2. Settings

Help Center

Logout

3. Deactivate your account

If you aren't able to deactivate your account using the steps above:

- Please contact us from the email address on your Student account and select "Wrong Account Type/ Deactivating an Account." If you do not have an email address on your Student account, you can add one on your Account Settings page.
- Make the subject line: "Delete Student Account" to request the deletion of your account.

2) Online learning platform – Coursera

If you don't want to use your Coursera account anymore, you can delete your account.

If you just want to stop getting emails from Coursera, you can change your email settings.

To delete your account:

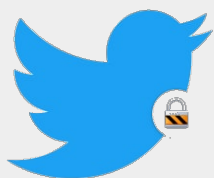
- Log into your Coursera account
- Open the drop-down menu at the top right
- Click Settings
- Click Delete Account at the bottom of the page

If you delete your Coursera account, you may not be able to restore your old account information. You'll need to create a new account to use Coursera again.

3) Social networking – twitter

- a) Click on Settings and privacy from the drop-down menu under your profile icon.
- b) From the Account tab, click on Deactivate your account at the bottom of the page.
- c) Read the account deactivation information, then click Deactivate @username.
- d) Enter your password when prompted and confirm that you want to proceed by clicking the Deactivate account button.

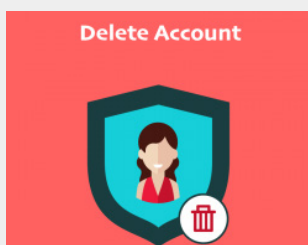
Further Reading



1) Protect Your Tweets with Twitter's New Privacy and Data Options

In this recent article, we looked at how you can protect your children's social media accounts, making sure that only their friends can see what they post and interact with them. We covered a number of major social media apps, such as Facebook, Instagram, WhatsApp, and more.

Link: <https://www.intego.com/mac-security-blog/protect-your-tweets-with-twitters-new-privacy-and-data-options/>



2) Make These 4 Changes Before You Delete Any Online Account

While surfing the Web, it's second nature to register on various websites in order to gain access to a variety of services, features, and goodies. Once the mystery is solved, you move on to something newer and shinier, leaving behind a trail of unused accounts. Get rid of clutter like that for a better digital life.

Link: <https://www.makeuseof.com/tag/make-4-changes-delete-online-account/>



3) How to Delete a WeChat Account on Android

This wikiHow teaches you how to permanently delete your WeChat account and all of your chat history using Android.

Link: <https://www.wikihow.com/Delete-a-WeChat-Account-on-Android>



4) Delete or Deactivate – What to do with your old accounts

When you stop using a social networking profile or website it's a good idea to deactivate or delete your account. This will mean that your content is no longer live and should not be searchable online; it will also remove the risk of these accounts being used by others or hacked without you knowing.

Link: <https://www.childnet.com/blog/delete-or-deactivate-what-to-do-with-your-old-accounts>



5) How to Delete Online Accounts You No Longer Need

Having too many digital accounts raises your risk of data being misused or stolen. Here's how to clean house.

Link: <https://www.consumerreports.org/privacy/how-to-delete-online-accounts-you-no-longer-need/>

Conclusion

Online learning is gradually becoming a basic learning method for everyone, especially during the period of COVID-19 pandemic. During online learning, data are collected, and data privacy and data security should be awarded by personal users. It is urgent to master basic skills for learners to protect their personal data and privacy in online learning.

In this guidance book, the definitions of several terms associated with personal data, privacy and online learning are analyzed, and the legislation and regulation on personal data protection from different countries and international organizations are presented. The relationship between personal data, student data, student privacy is discussed, the privacy frameworks and principles to be observed for online learning is listed, and the students' and parents' rights for data collected in online learning is also analyzed.

Based on the analysis, this guidebook identified the following five aspects of online learning relating to protect personal data and privacy protection.

1) Preparing devices and tools before online learning. Setting up the devices, managing the network settings, selecting and installing tools before online learning to ensure a solid learning environment is the basis for personal data protection. Multiple suggestions and solutions on these issues are presented in the guidebook.

2) Preserving personal data when logging in learning platforms. Registering and logging into learning platforms require learners to create a solid password, protect the password and biometric information to make a safe online learning environment. Specifically, when registering and logging on the public computer, the special notice should be taking on not saving login information, not leaving computer unattended with sensitive information on the screen, erase the tracks, disable the features of storing password, etc.

3) Protecting personal privacy when navigating learning platforms. For joining in the courses in LMS, utilizing personal learning services, using search engines, recognizing local services during online learning, specific solutions and practical steps are articulated in the part. How to back up the important data is also discussed in the section,

4) Keeping personal data safe when using social networking tools for learning. When using social networking tools, attention should be paid on utilizing webinar appropriately, posting in threaded discussion and forums responsibly, and surfing online safely, and concrete suggestions are provided for the issues.

5) Clearing personal data after finishing online learning. After finishing online learning, learner should make the decision on whether to delete the data or not. Suggestions and methods on how to delete the data and deactivate personal account are discussed in the section.

The book aims to provide guidance on protecting personal data during online learning, as online learning or blended learning has become a popular learning paradigm. The following five issues should receive the attention due.

1) The value of online learning should be noticed. "Ensure inclusive and equitable quality education and promote lifelong learning opportunities for all" is a sustainable development goal for 2030 agenda. Online learning is

the basic method to construct the roadmap to achieve this educational goal, not only during the period of educational emergency, but also for the period of post pandemic and the future.

2) The personal privacy protection should be promoted. The basic literacy on personal data protection during learning online, such as setting up devices, signing in LMSs, navigating learning platforms, are important for personal data security. In order to promote the protection of personal privacy in online learning, government's policy standards, industry's technology security system, and other stakeholders' actions should collectively build a safety environment for online learning.

3) Learning online could be regarded as an important way to prepare digital citizen. A digital citizen has the knowledge and skills to effectively use digital technologies to communicate with others, participate in society and create and consume digital content. Online learning has become a typical learning scenario for students, and the online learning behavior, habits, and ideas will definitely affect their life. Guiding learners participate in an appropriate manner in online learning could prepare ready, purposeful, and skilled digital citizens.

4) Collaboration skills could be drilled by cooperative learning in cyberspace. Individuals make meanings through the interactions with each other and with the environment they live. Online learning is not just to browsing contents, but to interacting with contents, peers, teachers and the environments. Therefore, students could utilize tools and techniques to communicate with peers and teachers in cyberspace, and at the same time understand how to protect their personal data in the communication process.

5) Digital learning could be infused with traditional education for flexible learning. Students could learn with free choices of times and location, digital resources, instructional approaches, learning activities, and supports services, which is the near future's flexible learning paradigm. The infusion of digital learning and traditional learning is the guarantee for flexible learning. The study of the infusion, including the personal data protection in the process, should be shared to bring a bright future for the mankind.

Reference

- Aarhus University. (2020). Types of personal data. Retrieved from <https://medarbejdere.au.dk/en/informationsecurity/data-protection/general-information/types-of-personal-data/>
- Acronis. (n.d.). Data Backup – What is it? Retrieved from <https://www.acronis.com/en-us/articles/data-backup/>
- Amazon. (n.d.). Close Your Account. Retrieved from <https://www.amazon.com/gp/help/customer/display.html?no-deId=GDK92DNLSGWT6MP>
- Anderson, T. (2011). The theory and practice of online learning (2nd Edition). Edmonton, AB: AU Press.
- Androws, T. (2019). How to Delete or Deactivate an Instagram Account [2020]. Retrieved from WaFtr: <https://www.waftr.com/delete-instagram-account/>
- Apple. (n.d.). iPhone Theft and Loss Claims. Retrieved from <https://support.apple.com/iphone/theft-loss-claims>
- Automatad. (2020). Consent Management Platform – Everything You Need to Know. Retrieved from: <https://head-erbidding.co/consent-management-platform-cmp>
- AWAKE. (n.d.). Network Intrusion. Retrieved from <https://awakesecurity.com/glossary/network-intrusion/>
- AWAKE. (n.d.). Sophistication and Power Comes Built In. Retrieved from <https://awakesecurity.com/product/>
- Baron, S. (2020). How to Back Up Data. Retrieved from wikiHow: <https://www.wikihow.com/Back-Up-Data>
- Bloom, A., Attai, L.(2016). The ABCs of Student Data Privacy. America: McGraw-Hill Education.
- Bodenham, L. (2017). How to manage your passwords safely. Retrieved from University of London: <https://london.ac.uk/news-opinion/london-connection/top-tip/manage-passwords>
- Brotherton, C. (2017). Is Your Website GDPR Compliant? How to Get Ready for the General Data Protection Regulations. Retrieved from wpmudev: <https://premium.wpmudev.org/blog/gdpr-compliance/>
- CANVAS. (2013). Day Five: Synchronous Learning Activities. Retrieved from <https://learn.canvas.net/courses/45/pages/day-five-synchronous-learning-activities>
- ChildnetInternational. (2018). Staying safe online whilst livestreaming - advice for parents and carers. Retrieved from <https://www.childnet.com/blog/staying-safe-online-whilst-livestreaming>
- Clarip. (2019). CCPA – Definition of Personal Information in California’s Privacy Law. Retrieved from <http://www.clarip.com/data-privacy/pi-definition-ccpa/>
- Committee of Ministers. (2010). the 1099th meeting of the Ministers’ Deputies. Retrieved from <https://search.coe>.

int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00

Common Sense. (2018). How can teachers and students better protect their online privacy? Retrieved from <https://www.commonsense.org/education/teaching-strategies/protect-your-students-data-and-privacy>

Common Sense. (2018). How can teachers and students better protect their online privacy? Retrieved from <https://www.commonsense.org/education/teaching-strategies/protect-your-students-data-and-privacy>

CommonSpaces. (n.d.). Registration and authentication. Retrieved from <https://www.commonspaces.eu/en/help/register/>

Coursera. (n.d.). Delete your Coursera account. Retrieved from <https://learner.coursera.help/hc/en-us/articles/209818563-Delete-your-Coursera-account>

Coursera. (2019). how to delete my question? Retrieved from <https://coursera.community/community-help-questions-40/how-to-delete-my-question-5289?postid=13141#post13141>

Coursera. (n.d.). Leave your organization's learning program. Retrieved from <https://learner.coursera.help/hc/en-us/articles/115001621606-Leave-your-organization-s-learning-program>

CUCU, P. (2016). 17 Underused Online Shopping Security Tips. Retrieved from HEIMDAL SECURITY : <https://heimdalsecurity.com/blog/online-shopping-security-tips/>

Data Quality Campaign. (2015). What Is Student Data? Retrieved from <https://dataqualitycampaign.org/resource/what-is-student-data/>

Data Quality Campaign. (2016). Why Education Data? Retrieved from <https://dataqualitycampaign.org/why-education-data/>

Doneda, D. (n.d.). Privacy and Data Protection Frameworks in the 21st Century. An interview to Danilo Doneda. (UNESCO, Interviewer)

EcomSpark. (2019). How to deactivate or delete Facebook Account? Retrieved from <https://www.ecomspark.com/how-to-deactivate-facebook-account/>

Edmodo. (2016). Browse and Follow Communities (Teacher). Retrieved from <https://support.edmodo.com/hc/en-us/articles/205009224-Browse-and-Follow-Communities-Teacher->

Edmodo. (2019). Delete a Post (Student). Retrieved from <https://support.edmodo.com/hc/en-us/articles/205006664-Delete-a-Post-Student->

Edmodo. (2019). Delete a Post (Teacher). Retrieved from <https://support.edmodo.com/hc/en-us/articles/205006474-Delete-a-Post-Teacher->

Edmodo. (2020). Deactivate a Student Account. Retrieved from <https://support.edmodo.com/hc/en-us/articles/205011954-Deactivate-a-Student-Account>

Edmodo. (n.d.). Communities and Topics. Retrieved from <https://support.edmodo.com/hc/en-us/sec>

tions/200910674-Communities-and-Topics

ElectronicFrontierFoundation. (2006). Six Tips to Protect Your Search Privacy. Retrieved from <https://www.eff.org/wp/six-tips-protect-your-search-privacy>

Erika. M., Tim. G., Karen. S. (2010). Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). America: NIST.

EUROPEAN DATA PROTECTION SUPERVISOR. (2020). Rights of the Individual. Retrieved from https://edps.europa.eu/data-protection/our-work/subjects/rights-individual_en

Facebook. (n.d.). How do I delete a video I posted on Facebook? Retrieved from https://en-gb.facebook.com/help/iphone-app/725107141317608?helpref=platform_switcher

Facebook. (n.d.). How do I remove something posted on my Facebook timeline? Retrieved from <https://en-gb.facebook.com/help/261211860580476/>

FEDERAL TRADE COMMISSION. (2017). Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business. Retrieved from <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance>

Flaherty, D. (1989). Protecting privacy in surveillance societies: The federal republic of Germany, Sweden, France, Canada, and the United States. Chapel Hill, U.S.: The University of North Carolina Press.

Francis, K. (2018). Major Goals And Expectations Of eLearning. Retrieved from elearningINDUSTRY: <https://elearningindustry.com/goals-and-expectations-of-elearning-major>

Gallagher, K., Magid, L., Pruitt, K. (n.d.). The Educator's Guide to Student Data Privacy. America.

GCFGGlobal. (n.d.). Google Account - Creating a Google Account. Retrieved from: <https://edu.gcfglobal.org/en/googleaccount/creating-a-google-account/1/>

Google. (2019). Helping kids be safe, confident explorers of the online world. Retrieved from https://beinternetawesome.withgoogle.com/en_us/

Google. (n.d.). Delete your Google Account. Retrieved from <https://support.google.com/accounts/answer/32046?hl=en>

Help Center. (n.d.). How to deactivate your account. Retrieved from <https://help.twitter.com/en/managing-your-account/how-to-deactivate-twitter-account>

Huang, R.H., Liu, D.J., Tlili, A., Yang, J.F., Wang, H.H., et al. (2020). Handbook on Facilitating Flexible Learning During Educational Disruption: The Chinese Experience in Maintaining Undisrupted Learning in COVID-19 Outbreak. Beijing: Smart Learning Institute of Beijing Normal University.

HUCULAK, M. (2020). How to make a full backup of your Windows 10 PC. Retrieved from Windows Central: <https://www.windowscentral.com/how-make-full-backup-windows-10>

IAPP. (2017). Categories of Personal Data. Retrieved from <https://iapp.org/resources/article/categories-of-personal-data/>

IAPP. (2020). What does privacy mean? Retrieved from IAPP: <https://iapp.org/about/what-is-privacy/>

IDENTITYGUARD. (2017). How Your Old Phone Number is Putting You at Risk. Retrieved from <https://www.identityguard.com/news/old-phone-number-putting-risk>

IEEE. (2016). IEEE Announces Standards Project Addressing Data Privacy Processes and Methodologies. Retrieved from https://standards.ieee.org/news/2016/ieee_p7002.html

i-scoop. (n.d.). Data subject rights and personal information: data subject rights under the GDPR. Retrieved from <https://www.i-scoop.eu/gdpr/gdpr-personal-data-identifiers-pseudonymous-information/>

ISO. (2011). ISO/IEC 29100:2011(en) Information technology — Security techniques — Privacy framework. Retrieved from <https://www.iso.org/standard/45123.html>

IT Governance. (n.d.). The GDPR and Privacy Compliance Frameworks. Retrieved from <https://www.itgovernance.co.uk/gdpr-privacy-compliance-framework-and-standards>

Karnes, K. (2020). Push Notification Best Practices: 35 Tips for Dramatically Better Messages. Retrieved from CleverTap: <https://clevertap.com/blog/push-notification-best-practices/>

KNOWLEDGE@WHARTON. (2019). Your Data Is Shared and Sold...What's Being Done About It? Retrieved from <https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/>

Knowliah. (2018). Categories of data in GDPR. Retrieved from <https://www.knowliah.com/en/learn/categories-of-data-in-gdpr>

Kowalski, P. (2017). If You Want Personalized Learning, Don't Forget about Data. Retrieved from Data Quality Campaign: <https://dataqualitycampaign.org/want-personalized-learning-dont-forget-data/>

Lam, J. (2019). How to protect your personal data? Retrieved from lawinfographic: <https://www.lawinfographic.com/protect-personal-data/>

learning-styles-online. (n.d.). Overview of Learning Styles. Retrieved from <https://www.learning-styles-online.com/overview/>

Lloyd, J. (2020). How to Block Adult Sites. Retrieved from wikiHow: <https://www.wikihow.com/Block-Adult-Sites#On-Windows-10>

Maciej. Z., Michal. W. (2018). What Is a Consent-Management Platform (CMP) and How Does It Work? Retrieved from CLEARCODE: <https://clearcode.cc/blog/consent-management-platform/>

Martinelli, K. (2018). Password Security Guidance. Retrieved from High Speed Training: <https://www.high-speedtraining.co.uk/hub/password-security-guidance/>

MatuszewskaKarolina. (2020). Comparison of 5 Leading Consent Management Platforms. Retrieved from: PIWIK:

<https://piwik.pro/blog/consent-management-platforms-comparison/>

Mikroyannidis, A. (2011). Supporting Self-Regulated Learning within a Personal Learning Environment: The Open-Learn case study. IEEE, (pp. 607-608).

Morin, A. (n.d.). Personalized Learning: What You Need to Know. Retrieved from Understood: <https://www.understood.org/en/school-learning/partnering-with-childrens-school/instructional-strategies/personalized-learning-what-you-need-to-know>

Nield, D. (2019). How to switch phones without losing anything. Retrieved from PopularScience: <https://www.pops-ci.com/switch-to-new-phone/>

NIST. (2017). Standards and Guidance Cited in NIST Privacy Framework RFI Responses. America.

Norton. (n.d.). How safe is surfing on 4G vs. WiFi? Retrieved from: <https://us.norton.com/internetsecurity-wifi-how-safe-is-surfing-on-4g-vs-wi-fi.html>

NortonLifeLock. (n.d.). Dangers of Free Downloads. Retrieved from <https://www.nortonsecurityonline.com/security-center/dangers-of-free-downloads.html>

OECD. (2013). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Retrieved from <https://www.oecd.org/internet/ieconomy/oecdguidelinesonthe protection of privacy and transborder flows of personal data.htm>

OFC. (2018). Protecting your privacy online. Retrieved from <https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/protecting-your-privacy-online/>

ORCID. (2019). Deactivating an ORCID account. Retrieved from <https://support.orcid.org/hc/en-us/articles/360006973813-deactivating-an-orcid-account>

Owyang, J. (2008). Understanding the difference between Forums, Blogs, and Social Networks. Retrieved from <https://web-strategist.com/blog/2008/01/28/understanding-the-difference-between-forums-blogs-and-social-networks/>

Panda. (2019). 8 Mobile Security Tips to Keep Your Device Safe. Retrieved from <https://www.pandasecurity.com/mediacenter/panda-security/mobile-security-tips/>

Pappas, C. (2016). eLearning Authoring Tool Costs: 7 Factors To Consider. Retrieved from elearningINDUSTRY: <https://elearningindustry.com/elearning-authoring-tool-costs-7-factors-consider>

PMaria. (2020). GDPR Privacy Policy Template. Retrieved from: PrivacyPolicies: <https://www.privacypolicies.com/blog/gdpr-privacy-policy>

Popescu, E., Ghita, D. (2013). Using Social Networking Services to Support Learning. Romania: Craiova University.

Privacy Technical Assistance Center. (2014). Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices. America.

PrivacyPolicies. (2020). Privacy Policies are Legally Required. Retrieved from https://www.privacypolicies.com/blog/privacy-policies-legally-required/#What_Is_A_Privacy_Policy

PrivacySense. (2016). Personal Information. Retrieved from <http://www.privacysense.net/terms/personal-information/>

ProtectingStudentPrivacy. (n.d.). What is an education record? Retrieved from <https://studentprivacy.ed.gov/faq/what-education-record>

ROBINSON, R. (2020). Data Privacy Vs. Data Protection. Retrieved from Ipswitch: <https://blog.ipswitch.com/data-privacy-vs-data-protection>

SafeOnline. (n.d.). How to Prevent Cell Phones From Being Tracked. Retrieved from <https://safeonline.ng/communications/how-to-prevent-cell-phones-from-being-tracked/>

SCORM. (n.d.). SCORM Explained 201: A deeper dive into SCORM. Retrieved from https://scorm.com/scorm-explained/?utm_source=google&utm_medium=natural_search

SecureControlsFramework. (2018). Secure Controls Framework (SCF) Privacy Management Principles.

SHAD, A. (2018). Top 10 Free GDPR Tools and Solutions You Didn't Know Before. Retrieved from ECOMPLY.io: <https://ecomply.io/top-10-free-gdpr-tools-and-solutions/>

Student Data Principles. (n.d.). 10 Foundational Principles for Using and Safeguarding Students' Personal Information. Retrieved from <https://studentdataprinciples.org/the-principles/>

STUDENTPRIVACYPLEDGE. (2015). K-12 School Service Provider Pledge to Safeguard Student Privacy. America.

TechTarget. (2007). hijacking. Retrieved from <https://searchsecurity.techtarget.com/definition/hijacking>

TEKETEIPURANGI. (2018). Choosing the right digital device. NewZealand.

The Western PA Healthcare News Team. (2017). Social Network Etiquette: How to Mind Your Manners Online. Retrieved from HealthcareNews: <https://www.wphealthcarenews.com/social-network-etiquette-mind-manners-online/>

Toledo, R. (n.d.). How to Protect Your Privacy on Your Mobile Devices. Retrieved from Lifehack: <https://www.lifehack.org/articles/technology/how-protect-your-privacy-your-mobile-devices.html>

Triella. (2018). WEAK PASSWORDS ARE STILL THE BIGGEST SECURITY RISK. Retrieved from <https://www.triella.com/weak-passwords/>

Twitter. (n.d.). How to delete a Tweet. Retrieved from <https://help.twitter.com/en/using-twitter/delete-tweets>

Wan, T. (2017). How to Protect Education Data When No Systems Are Secure. Retrieved from EdSurge: <https://www.edsurge.com/news/2017-09-25-how-to-protect-education-data-when-no-systems-are-secure>

Wikipedia. (2020). Information privacy law. Retrieved from https://en.wikipedia.org/wiki/Information_privacy_law

Wikipedia. (2020). Personal data. Retrieved from https://en.wikipedia.org/wiki/Personal_data

Wikipedia. (2020). Sharable Content Object Reference Model. Retrieved from https://en.wikipedia.org/wiki/Sharable_Content_Object_Reference_Model

WorldEconomicForum. (n.d.). Personal Data: The Emergence of a New Asset Class. Retrieved from <https://www.weforum.org/reports/personal-data-emergence-new-asset-class>

Zhan. T., Wang. X. (2020). Personal Data Security Technical Guide for Online Education Platforms. Retrieved from the UNESCO Institute for Information Technologies in Education: <https://iite.unesco.org/publications/personal-data-security-technical-guide-for-online-education-platforms/>

Glossary

Online learning (1.1)

Online learning is defined as learning experiences in synchronous or asynchronous environments using different devices (e.g., mobile phones, laptops, etc.) with internet access. In these environments, students can be anywhere (independent) to learn and interact with instructors and other students (Singh and Thurman, 2019).

Personally Identifiable Information (PII) (2.1)

Personally Identifiable Information (PII) is —any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

– *NIST SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*

Education record (2.2)

“Education records” are records that are directly related to a student and that are maintained by an educational agency or institution or a party acting for or on behalf of the agency or institution. These records include but are not limited to grades, transcripts, class lists, student course schedules, health records (at the K-12 level), student financial information (at the postsecondary level), and student discipline files. The information may be recorded in any way, including, but not limited to, handwriting, print, computer media, videotape, audiotape, film, microfilm, microfiche, and e-mail.

– *34 CFR § 99.2, Family Educational Rights and Privacy Act of United States*

Privacy (2.2)

Privacy is the tranquility of the private life of a natural person, and the private space, private activities, and private information that one is unwilling to be known to others.

– *Article 1032, Civil Code of the People's Republic of China*

Privacy policy (2.3)

A privacy policy is a statement or a legal document (in privacy law) that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data. Personal information can be anything that can be used to identify an individual, not limited to the person's name, address, date of birth, marital status, contact information, ID issue, and expiry date, financial records, credit information, medical history, where one travels, and intentions to acquire goods and services.

– *McCormick, Michelle. “New Privacy Legislation.” Beyond Numbers 427 (2003): 10-. ProQuest. Web. 27 Oct. 2011*

Wi-Fi (3.2)

Wi-Fi is a technology for electric devices to connect to a wireless local area networking (WLAN). Wi-Fi is usually referred to as wireless network.

Virtual Private Network (VPN) (3.2)

A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated circuits or with tunneling protocols over existing networks.

Secure Socket Layer (SSL) (3.3)

SSL is a security protocol implemented on top of TCP/IP protocols. SSL supports various network and it provides three basic security services, all of which are enabled by a public key and a symmetric key.

Uniform Resource Locator (URL) (4.1)

A Uniform Resource Locator (URL), colloquially termed a web address, is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.

Learning management system (LMS) (5)

A learning management system (LMS) is a software application for the administration, documentation, tracking, reporting, automation and delivery of educational courses, training programs, or learning and development programs.

– Ellis, Ryann K. (2009), *Field Guide to Learning Management, ASTD Learning Circuits*, archived from the original on 24 August 2014, retrieved 5 July 2012

(Web) Search engine (5.3)

A search engine is a term commonly used to refer to a web search engine. A web search engine or Internet search engine is a software system that is designed to carry out web search (Internet search), which means to search the World Wide Web in a systematic way for particular information specified in a textual web search query. The search results are generally presented in a line of results, often referred to as search engine results pages (SERPs).

HTTP cookie (5.3)

An HTTP cookie (also called web cookie, Internet cookie, browser cookie, or simply cookie) is a small piece of data sent from a website and stored on the user's computer by the user's web browser while the user is browsing.

Location-based service (LBS) (5.4)

A location-based service (LBS) is a general term denoting software services which utilize geographic data and information to provide services or information to users. LBS can be used in a variety of contexts, such as health, indoor

object search, entertainment, work, personal life, etc.

Social network and Social networking service (6)

A social network is a social structure made up of a set of social actors (such as individuals or organizations), sets of dyadic ties, and other social interactions between actors. The social network perspective provides a set of methods for analyzing the structure of whole social entities as well as a variety of theories explaining the patterns observed in these structures.

– Wasserman, Stanley; Faust, Katherine (1994). *“Social Network Analysis in the Social and Behavioral Sciences”*. *Social Network Analysis: Methods and Applications*. Cambridge University Press. pp. 1–27. ISBN 9780521387071.

A social networking service (also social networking site or social media) is an online platform which people use to build social networks or social relationships with other people who share similar personal or career interests, activities, backgrounds or real-life connections.

Domain Name System (DNS) (6.3)

The Domain Name System (DNS) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities.

Index of Topics

Chapter 3 Preparing Devices, Network, and Tools	3.1 Setting up your device	Level Know/Vigilant/Protect yourself/Protect others	Topic What online learning devices can I choose?
		Related User Students, Parents, Teachers	
		Related User Students, Parents, Teachers	Topic How can I keep my device safe?
		Risks - Loss or Theft - Abandonment or Switch	
	3.2 Managing network connection on your device	Level Know/Vigilant/Protect yourself/Protect others	Topic How to connect mobile devices to the Internet?
		Related User Students, Parents, Teachers	
		Related Privacy Personal data stored in devices such as personally identifiable information	
		Risks - Network Intrusion - Man-in-the-Middle Attack - Browser Hijacking	Topic How can I use the Internet safely?
	3.3 Selecting and installing learning tools	Level Know/Vigilant/Protect yourself/Protect others	Topic How do I, as a teacher, select tools for my students?
		Related User Students, Parents, Teachers	Topic How do I safely download and install software?
		Related Privacy Personally Identifiable Information, biometric information	
		Risks - Fake or Malicious Websites - Computer Viruses - Malicious Software	

Chapter 3 Preparing Devices, Network, and Tools	3.4 Browsing the privacy policy	Level Know/Vigilant	Topic Where to find the privacy policy?
		Related User Students, Parents, Teachers	
		Related Privacy Basic information	
		Risks Misuse of data by online learning tools	
Chapter 4 Preserving Privacy when Signing up on Learning Platforms	4.1 Using strong password to create account	Level Know/Vigilant/Protect yourself	Topic How do I create a strong password?
		Related User Students, Parents, Teachers	Topic Use password management tools
		Related Privacy Personally Identifiable Information, network identity information	Topic How to generate strong password with google chrome or iOS?
			Topic How do I protect my passwords from leaking?
		Risks - Weak Passwords - Password Leak	Topic What are biometric identifiers?
			Topic How can I protect my biometric information?
	4.2 Signing in a device that's not yours	Level Know/Vigilant/Protect yourself	Topic How to use a public computer safely?
		Related User Students, Parents, Teachers	
		Related Privacy Personally Identifiable Information, network identity information	
		Risks User Information Leakage	

Chapter 5 Protecting Privacy when Navigating Learning Platforms	5.1 Enrolling in an online course	Level Know/Vigilant/Protect yourself	Topic How to enroll in an course? (Coursera for example)
		Related Users Students, Parents	Topic How to browse and follow communities? (Edmodo for example)
		Related Privacy Basic information, attendance information, preferred content, study records	
		Risks Data leak due to user, site or third parties.	
	5.2 Utilizing personalized learning services	Level Protect yourself	Topic What policymakers and education leaders need to know when developing a variety of strategies to personalize learning?
		Related Users Students	
		Related Privacy Personal internet history	
		Risks - Extraction and malicious use of information such as user preferences and learning patterns - User information leakage due to outside attack on platforms - Illegal information provision to third-party platforms	
	5.3 Using search services carefully	Level Protect yourself	Topic How to protect your search privacy?
		Related Users Students	
		Related Privacy Internet browsing traces	Topic How to block “cookies” from your search engine?
		Risks - Extraction and malicious use of information such as user preferences and learning patterns - User information leakage due to outside attack on platforms - Illegal information provision to third-party platforms	

Chapter 5 Protecting Privacy when Navigating Learning Platforms	5.4 Recognizing location services	Level Know/Vigilant/Protect yourself	Topic How to prevent cell phones from being tracked?
		Related Users Students	
		Related Privacy Personal location information	
		Risks - Threats to personal and property safety caused by location information leakage - User information leakage due to outside attack on platforms - Illegal information provision to third-party platforms	
	5.5 Backing up your data	Level Know/Vigilant/Protect yourself	Topic How to make a data backup?
		Related Users Students, parents, teachers	
		Related Privacy Personally Identifiable Information, etc.	
		Risks - Reselling of personal information - Advertisements - Life safety	
Chapter 6 Staying Safe while Learning with Social Networking	Topic What should I consider in social network?		
	Topic How to use social networking services as learning tools?		
	6.1 Using video conference tools with caution	Level Know/Vigilant/Protect yourself/Protect others	Topic Staying safe online whilst livestreaming - advice for parents and carers
		Related Users Students, Parents, Teachers	
		Related Privacy Personally Identifiable Information, personal property information, personal location information	
		Risks - Live pictures containing personal identifiable information, personal location information, personal property information etc. - User information leakage due to outside attack on platforms - User information leakage due to outside attack on personal devices	

Chapter 6 Staying Safe while Learning with Social Networking	6.2 Posting in forums responsibly	Level Know/Vigilant/Protect yourself/Protect others	Topic Social network etiquette: How to mind your manners online?
		Related Users Students, Parents, Teachers	
		Related Privacy Personally Identifiable Information, personal property information, personal information location	
		Risks - Extraction and malicious use of information such as user preferences - User information leakage due to outside attack on platforms - Illegal information provision to third-party platforms	
	6.3 Surfing the Internet safely	Level Know/Vigilant/Protect yourself	Topic How to block inappropriate content?
		Related Users Students	Topic How to manage your push notifications?
		Related Privacy Personal internet history	
		Risks - Extraction and malicious use of information such as user preferences - User information leakage due to outside attack on platforms - Illegal information provision to third-party platforms	
Chapter 7 Clearing Personal Data after Learning Online	7.1 Removing data traces in online learning	Level Know/Vigilant/Protect yourself	Topic How to delete user-generated content?
		Related Users Students	
		Related Privacy Personally Identifiable Information, personal internet history	
		Risk - The platform did not give permission to delete - Illegal retention of information after deleting	
	7.2 Deactivating your account	Level Know/Vigilant/Protect yourself	Topic How to deactivate an account?
		Related Users Students	
		Related Privacy Personally Identifiable Information, personal internet history	
		Risks - The platform does not permit to deactivate - Illegal retention of information after deactivating	



北京师范大学智慧学习研究院
Smart Learning Institute of Beijing Normal University

Website: <http://sli.bnu.edu.cn/en/>

Address: 12F, Block A, Jingshi Technology Building,
No. 12 Xueyuan South Road, Haidian
District, Beijing, China

Email: smartlearning@bnu.edu.cn

Phone: 8610-58807219

Postcode: 100082



<http://sli.bnu.edu.cn/en>